SECURITY AND USABILITY IN PASSWORD AUTHENTICATION

MERVE YILDIRIM

Foundation of Software Systems

Department of Informatics

University of Sussex

A thesis submitted, on April 2017, in partial fulfilment of the requirements for the degree of Doctor of Philosophy (PhD) in the School of Engineering and Informatics of the University of Sussex.

Signed Declaration

I hereby declare that this thesis has not been and will not be, submitted in whole or in part to another University for the award of any other degree.

Signature: .....

MERVE YILDIRIM

12th April 2017

Dedicated to my dear parents

and

wonderful sister and brother

UNIVERSITY OF SUSSEX

MERVE YILDIRIM

THESIS SUBMITTED FOR THE DEGREE OF DOCTOR OF PHILOSOPHY (PhD)

SECURITY AND USABILITY IN PASSWORD AUTHENTICATION

ABSTRACT

This thesis investigates the human-factor problems in password authentication and proposes some usable solutions to these problems by focusing on both forms of knowledge based authentication: textual passwords and graphical passwords. It includes a range of empirical studies to examine users' password-related behaviour and practices in authentication, and helps users to adopt secure password behaviour.

This thesis consists of two parts. The first part focuses on traditional text-based passwords. Design flaws and usability issues of existing text-password mechanisms used by many organisations cause employees to adopt insecure password practices. The first work in this thesis investigates the reasons for employees' lack of motivation regarding password protection against security failures. An empirical study is conducted to identify the factors causing employees' insecure behaviours in organisations, and several persuasion strategies are tested to persuade employees to use passwords more safely. The results of the study revealed that some persuasion strategies are effective in motivating users to adopt good password practices. The study also found that the failure of password policies and authentication schemes deployed by organisations is a common problem among the organisations.

Considering the results of the first study, in the second work of this thesis, a password guideline/advice study is conducted to help users to create stronger and more memorable passwords. A password guideline including a number of password creation methods and a persuasive message is proposed, and its effectiveness in improving the strength of user-

chosen passwords is evaluated. The results show that the users who received the proposed guideline produced stronger and more memorable passwords than the users followed the usual password restrictions while creating their passwords. The results also demonstrate that the given password creation methods can be helpful and inspirational for users to create their own encryption formula.

All these works reveal the weaknesses of user-chosen textual passwords and inefficacy of existing text-based password mechanisms. Although these studies show that text-based password mechanisms can be strengthened, they are still problematic where usability is concerned. Thus, the second part of this thesis focuses on another form of knowledge-based authentication: graphical passwords. A novel hybrid authentication scheme integrating text and images is introduced to minimise the brute force and shoulder surfing attacks which text and graphical passwords suffer. In the last work of this thesis, the proposed hybrid scheme is implemented and evaluated. The evaluation shows that the proposed scheme provides security and usability at the same time, and it also makes the password creation process enjoyable for users.

In summary, the thesis contributes to the analysis of some key security and usability problems which arise in knowledge-based authentication. A series of empirical studies has been conducted. Based on their results, usable solutions to the human-factor problems in password-based authentication are proposed and evaluated.

ACKNOWLEDGEMENT

First and foremost, I would like to thank my dear supervisor, Dr. Ian Mackie for his invaluable support, guidance and encouragement during my studies in the University of Sussex over the last four years. His knowledge and support has always been inspiring for me. Without his trust, this research would have never been achieved and completed.

I would like to thank Dr. Kate Howland, who kindly accepted to attend my all annual review meetings as a committee member and my viva as an internal examiner. Her valuable suggestions and constructive criticism helped me throughout my PhD studies. I would like to thank Dr. Richard Overill who attended my viva as an external examiner for his kindness and valuable comments and suggestions. I would also like to thank to another committee member of my annual review meetings, Dr. Natalia Beloff, for her valuable suggestions and guidance.

Special thanks to Yusuf Serdar Gokcenay, for his outstanding support, endless patience and invaluable friendship throughout my studies in University of Sussex. His support and encouragement kept me motivated all the time.

Many thanks to Paul Sanford who became like a grandfather to me during my life in UK. I will never forget his support, endless guidance and great helps during my studies. I would like to thank the Candan family for their hospitality and invaluable friendship during my life in UK. I would also like to thank psychiatrist Muge Ozvarol and computer scientist Tolga Ulucay for their valuable criticism and contributions to my studies.

Moreover, I would like to extend my thanks to the members and personnel of the Department of Informatics who always been helpful and supportive during my studies in University of Sussex.

Finally, I would like to thank my parents for their endless love, patience and prayers, and my sister and brother for their great support, encouragement and positive energy.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 INTRODUCTION

This chapter presents the general idea of the research; including the scope of the thesis, research questions and aims and objectives to find answers to those questions. It also briefly explains the research approach and the research methods used in the several empirical studies which are conducted to evaluate the proposed idea in this thesis. At the end of this chapter, the thesis contributions are presented and the organisation of the thesis is detailed.

1.2 RESEARCH BACKGROUND AND SCOPE

As information technology is an inevitable necessity in today's world, computer and information security has become critically important for many organisations. In computer systems, this issue has been mostly about ensuring confidentiality, integrity and accessibility to information. Because of the importance of the subject, numerous studies have been conducted in this area but unfortunately most of the researchers have primarily focussed on technical problems and solutions rather than human factors in information systems (Hoonakker, Bornoe and Carayon, 2009).

Human factors in security systems are often overlooked although this is one of the most important aspects of computer security. In recent years, researchers have started to pay attention to this subject and some studies have emerged to show the effect of the human role on computer and information security. Also, recently, the security research community has stated that users' behaviour plays an important role in many security failures (Cranor, 2008). Undesirable user behaviour causes the majority of the security failures in the organisations. There are many reported cases proving that user behaviours enabled or facilitated a security breach (Sasse, Brostoff and Weirich, 2001). The main reason for this situation is that end users generally have difficulties to understand

computer security properly. Computer security terms such as *encryption*, *public key, private key* or *phishing* or *pharming* techniques used in sophisticated attacks usually do not make any sense to most end users. This is not only about the complexity of the terms but also the proffered solutions to security problems are changing rapidly. End users are unable to cope (Zakaria, 2013).

One of the important points about complexity is to consider that computer security is often investigated as a *secondary task*. Most users find the security mechanisms too burdensome so they prefer to avoid security efforts in order to perform their *primary task*. There is mostly a contradiction between the user's idea of how the system works and how the system actually works which leads to making inappropriate security-related decisions. Users generally are not motivated to care about security because the effects or consequences of not behaving in a secure manner do not appear immediately. Therefore, they often only realize the situation after they have become the next victim of a security failure.

There are two main research areas in which user behaviour issues are being currently studied. The first one is *information security management* (ISM) which mainly focuses on some approaches such as education, training and security awareness programs (Woodhouse, 2007; Herath and Rao, 2009). Yet these approaches have not been a solution for motivating users to behave securely. The second area is *usable security* in which researchers have studied the inclusion of usability elements into security mechanisms to make users engage in the task more willingly (Schultz et.al, 2001; Zurko, 2005). Despite these efforts, there is still a gap in the Human Computer Interaction (HCI) field in terms of designing usable security mechanisms to improve users' motivation to adopt desired security behaviours.

Whitten and Tygar (1999) stated that PGP 5.0, one of the most popular encryption software used in the past, is not usable by average computer users because it has user interface design flaws. Since then, security researchers began to realize the importance of investigating human factors on security systems, and designing usable systems accordingly (Smith, 2003; Schenier, 2004).

User authentication is usually the first stage of a security sensitive system which users have to confront with to prove their right of access (Smith, 2001). There is an *identification* phase where the user claims that he/she is the person who has right to access the system and *authorization* phase where the user has to provide credentials to prove his/her claims (Renaud, 2005). The three differing authentications are *what the user has*, *who the user is* and *what the user knows* (Smith, 2001; Renaud, 2005). *What the user has* commonly imply the possession of a device such as digital authentication tokens or smart cards to prove the identity of users. These tokens are commonly used as security tools in enterprises. A research study about tokens and smart cards points out usability issues emerged from the need of installing drivers on a range of machines to support different forms of tokens and cards (Piazzalunga et.al, 2005). In terms of authentication, *who the user is* refers to biometrics which measure user's physiological or behavioural characteristics. Biometrics are considered the best solution since they give accurate results about the claimed identity thus provide high level security. However, in practice, they have many usability and security issues. Non-adaptation of some user groups to biometrics systems (Coventry, 2005), the possibility of imitation of some biometrics such as mocking finger prints using special materials and also affordability problems of these systems are some of aforementioned issues. *What the user knows* (often referred to as knowledge based authentication) typically requires the user remember a secret he/she created before and provide it when asked to gain access a system. Text-based password is the oldest and most commonly used type of knowledge based authentication. Text password is ubiquitous on the Internet since it is affordable, widely deployed, familiar to users and easy to replace.

Authentication, as one of the most important fields of computer security to allow authorized users to access information, has been studied by many usable security researchers. Various alternative authentication schemes to text-based passwords which aim at aligning security and usability, have been proposed so far. These proposals range from graphical password authentication to location-based authentication (Goldberg, Hagman and Sazaval, 2002; Forget, 2012; Thorpe, MacRae and Salehi-Abari, 2013). However, none of these schemes could overcome the simplicity and affordability of typing a sequence of keyboard characters to allow authenticating users (Bonneau, 2012). As a result, traditional text-based password is still the most popular authentication

mechanism on the Web, and it is likely to remain in the near future (Herley, Oorschot and Patrick, 2009).

Unfortunately, in terms of usability, text- based password authentication is quite problematic. A good password needs to be "easy to remember and hard to guess" at the same time, as suggested by Wiedenbeck et al. (2005a). However, passwords which are easy to remember are generally short and/or meaningful words, or slight variations. Therefore, these passwords become vulnerable to dictionary attacks. Passwords including personal information are also memorable, but they might be easily guessable especially by family members and friends.

A lot of work has been done to understand users' password behaviour and practices. A landmark study involving half a million users was conducted by Microsoft Research and many interesting findings about users' password habits were revealed (Florencio and Herley, 2007). Additionally, many researchers have focussed on password management, password guideline and advice issues and conducted laboratory studies, to understand the reasons behind particular password behaviours such as sharing or reusing passwords and to investigate possible security countermeasures (Gaw and Felten, 2006; Shay et al., 2010).

Considering the above-mentioned issues, this thesis aims to bridge the gap between password security and usability by focusing on human factor issues in the password authentication domain. As password security is one of the most important areas where human factors play a crucial role, it is important to investigate further the effect of user behaviour on password practices. Text passwords' popularity, despite their weaknesses, makes the subject more interesting to study in terms of user behaviours. The next section presents the research problems pertaining to password security.

1.3 RESEARCH PROBLEMS

Password authentication is nowadays the most commonly used authentication mechanism and it seems likely that it will continue to be so for many years to come. This is because it is widely deployed, easy to use, affordable and familiar to users. Passwords

are used to protect users' information in many platforms ranging from banking transactions to social networking sites. Thus, they play a key role in the protection of personal and financial information in online and offline environments.

Passwords are considered one of the most significant risk factors in terms of security in information systems as they are vulnerable to attacks (Carstens, Mc-Cauley and DeMara, 2004). This vulnerability is mainly due to the user behaviours and practices, not related to the password system itself. The main problem arises from the memorability issue which ultimately causes the other problems related to passwords such as reusing, sharing and choosing weak passwords. These problems are well-known and they are called as 'the human factor problems' by researchers in the password authentication domain (Herley, Oorschot and Patrick, 2009; Summers and Bosworth, 2004).

Most people are actually aware of the importance of choosing strong passwords to protect their information. However, there is a lack of password creation advice or guidelines to help and motivate them to compose strong passwords. It is commonly stated that a password should include a mix of keyboard characters and should not include the meaningful words from dictionaries (Yan et al., 2004). Similar advice can also be found in websites, policy papers and many other password security themed articles. Unfortunately, despite these guidelines and advice, most users do not adopt good security behaviours and care to choose strong passwords. Based on occurrences of security failures and the difficulty to determine which particular rules measure the importance or necessity of strong password creation, research shows that users commonly underestimate the risk associated with weak passwords. (Florencio and Herley, 2007; Zang and McDowell, 2009).

Shay et al. (2010) indicated that users often appear to lack motivation to produce strong passwords as they are not convinced of the importance of suggestions given in the guidelines. It was proved that users' awareness of the problems is not enough to restrain them from adopting undesirable security practices such as using dictionary words, sharing and reusing their passwords. So, more effective approaches are needed to convince users to behave in a secure manner in the password authentication domain. Probably, rather than only telling them why they should choose strong passwords or restricting their choices with tedious password policy rules, showing how to create better passwords in efficient and fun ways is more convenient.

1.4 RESEARCH QUESTIONS AND OBJECTIVES

From the issues mentioned above it is clear that the existing password guidelines and advice have not solved the problem of weak password creation. New techniques are needed to help users to create strong passwords by presenting new solutions which will make the password creation process more reasonable, interesting and fun. The new solutions must motivate and lead users to construct strong passwords and also show the consequences of bad password practices. Thus, this research aims to find out whether a change in password guidelines and advice can bring a new perspective for users and to improve their password security behaviour. Furthermore, since user behaviour issues are extremely complex as they are shaped according to different environments and conditions users have. Based on this point, this research also aims to include an experiment for users working in organisations to improve understanding of their security behaviours particularly related to password practices. Some chosen elements of *persuasion technologies* have been used to change users' undesirable password behaviours and convince them to adopt desired ones.

Although there should be efforts to persuade users to create strong passwords and abandon password sharing and reusing habits, the memorability problem will remain unchanged. To handle this problem, many studies have been conducted by researchers and various authentication mechanisms have been proposed in the industry. Among the mechanisms being proposed, a graphical password is the closest alternative to the traditional text-based password in terms of its implementation, affordability and easy usage. Various graphical password schemes recently emerged aiming to overcome the main weakness of traditional text-based (alphanumeric) passwords, which is memorability. They are indeed advantageous due to the fact that the human memory can recall graphical images better than text and numbers.

Despite their advantages, since graphical passwords are still not commonly used, further investigation is needed to find out whether they can completely replace the text-based passwords, or can only help to strengthen existing defences to attacks. Similar to other alternatives, graphical password schemes have many downsides particularly with regards to its weakness to spyware and shoulder surfing attacks. Thus, designing new graphical schemes to strengthen its defence to these attacks is crucial before it becomes

more established. At this point, hybrid authentication mechanisms are seen convenient to minimize the downsides of traditional text-based passwords and graphical passwords and use the advantages of both. We have investigated the potential of a hybrid password scheme as an alternative mechanism. Hence, this research has proposed a novel hybrid password authentication scheme which has upsides of text-based passwords and graphical passwords to offer a better solution than existing ones. This thesis presents solutions to these problems.

The research questions guiding this research study are as below:

1- "How can password related behaviours, which may potentially lead to security failures, be changed to improve overall password security in organisations?"

2- "To what extent can users be directed and motivated to choose strong passwords through password advice?"

3- "Can graphical passwords entirely replace the textual passwords?"

4- "Can a hybrid password authentication scheme integrating text and graphical passwords be solution to the password security and usability problems?"

The purpose of this research is to investigate user security behaviour in the password authentication domain and to offer usable solutions to decrease security risks caused by these behaviours. For this purpose, these research questions will be answered by achieving some objectives. The main objectives and concomitant research activities to be carried out for each question are listed below:

Main Objectives:

1- Conducting a broad literature review to address the key issues of the research topic and to follow the related studies.
2- Identifying the research problems, questions and gaps in the research field.
3- Proposing solutions to the research questions specified.
4- Evaluating the proposed solutions.
5- Providing an overall discussion of the findings when conducting the research.

Research Activities Related to Each Research Question

1- "How can password related behaviours, which may potentially lead to security failures, be changed to improve overall password security in organisations?"

Research Activities (1):

- Reviewing the studies and cases on employees' security behaviour in password authentication in organisations.
- Examining the existing methods which aim to make employees adopt good security behaviours.
- Reviewing the related persuasion approaches and methods to change user behaviour.
- Applying the selected persuasion methods to change employees' behaviour so they behave in a secure manner.
- Conducting empirical studies to analyse these methods' efficiency.
- Drawing a conclusion from the results of the empirical studies.

2- "To what extent can users be directed and motivated to choose strong passwords through password advice?"

Research Activities (2):

- Reviewing relevant studies on password policy rules and password advice.
- Examining the existing password policies and guidelines.
- Proposing a new idea which may solve the problems with the existing systems.
- Conducting an empirical study to find out whether the new idea works better to direct and motivate users to choose strong passwords than existing solutions.
- Drawing a conclusion from the results of the empirical study.

3- "Can graphical passwords entirely replace the textual passwords?"

Research Activities (3):

- Reviewing the alternative authentication mechanisms to the traditional text password passwords and assessing the alternatives according to certain criteria.
- Examining the existing graphical password authentication schemes and deciding on the best alternative.
- Specifying the upsides and downsides of the decided scheme.
- Drawing a conclusion from the results of the research.

4- "Can a hybrid password authentication scheme integrating text and graphical passwords be solution to the password security and usability problems?"

Research Activities (4):

- Based on the results of the research done for previous question, proposing a novel hybrid password authentication scheme including text and graphical passwords.
- Designing a web application to apply the proposed authentication scheme.
- Conducting an empirical study to test the proposed authentication scheme.
- Evaluating the efficiency of the new scheme to find out whether it is convenient to use for users to create memorable and strong passwords.
- Drawing a conclusion from the evaluation.

An empirical study called *improving password security in organizations* which is presented in chapter 4 addresses the first research question. The password guideline-advice study called *persuading users to create stronger passwords* which is presented in chapter 5 addresses the second research question. Chapter 6 which is a background chapter reviewing the existing authentication mechanisms and comparing the graphical password schemes aims to find solution to third research question. The last empirical study called *evaluation of security and usability of a novel user authentication scheme integrating text and graphical passwords* which is presented in chapter 7 addresses the final research question. The details of the empirical studies and results are provided in the related chapters and overall discussion is presented in the last chapter.

1.5 RESEARCH APPROACH

This research study aims to investigate user security behaviour issues related to the password authentication domain and offer usable solutions to direct and motivate users to adopt desired behaviours. Thus, throughout this study, an empirical-based approach is adopted conducting three empirical studies to achieve the proposed research aim.

The first empirical study is conducting interviews and surveys with employees of big organisations to figure out the reasons behind bad password practices and find solutions to their lack of motivation to adopt good ones. A series of persuasion approach and methods have been reviewed and the selected ones have been used to convince and motivate users to avoid some security behaviours that put their personal information as well as the organisational information at risk. The study has been conducted in six organisations in Turkey including a hospital, a software company and a construction company. This involved 121 participants including IT managers, software specialists and other employees who do not have an IT background. The empirical study is detailed in Chapter 4.

The second empirical study is a "password guideline-advice study" that has been conducted to investigate whether providing users a series of useful password creation methods alongside a motivating rationale is more effective than strict policy rules in terms of creating strong and memorable passwords. The password advice and the password creation methods have been specified after a broad literature review was conducted. This empirical study involved 380 participants including university students from UK, USA and Turkey. Details of the password guideline- advice study are discussed in Chapter 5.

The third and final empirical study is evaluating a novel hybrid authentication scheme integrating text and graphical passwords. This novel authentication scheme has been designed after a broad literature review on alternative authentication mechanisms was conducted. This study involved 52 participants who are undergraduate and postgraduate students studying in the University of Sussex. Especially existing graphical password schemes were especially scrutinised, and eventually recall based graphical passwords were considered the best alternative to the traditional text-based passwords

considering certain criteria. The results of this study showed how a hybrid password authentication scheme can improve password strength by taking advantages of the upsides of text and graphical passwords as well as eliminating the vulnerabilities of both. The details of the study, including the usability and security evaluation, are discussed further in Chapter 7 of this thesis.

1.6 CONTRIBUTIONS

This thesis aims to address security problems caused by human factors in textual and graphical password authentication, and to propose solutions for these problems while maintaining usability. This endeavour is detailed in the thesis through the following contributions to the field of user authentication and usable security:

- A user study has been conducted with participants in several organisations from different sectors to understand the reasons for undesired password behaviour in password authentication. It gives interesting results that led us proposing different security solutions for different organisations as needs and ways to motivate users in each organisation vary. Persuasion Technology has been used to convince users in the organisations to adopt good password behaviour. At the end of the study, some recommendations for IT departments which can be useful in improving password security and decreasing the probability of security failures significantly is presented.

- A new user-friendly password guideline and advice for motivating and influencing users to select more secure and memorable text passwords without overburdening their memory. A broad user study has been conducted to evaluate the efficiency of these password guideline and advice. It has yielded good results which suggests that the password creation tips and persuasive message provided to users convinced them to create cryptographically strong and memorable passwords. Also, the study suggests that this new password guideline and tips are much more efficient than strict password policy rules regarding creation of strong passwords.

- Design and evaluation of a novel hybrid authentication scheme integrating text and graphical passwords. The proposed scheme is resistant to shoulder surfing attack, which is the main security problem of graphical passwords. Also, the new scheme is enjoyable

to use for users to motivate them to create strong but memorable passwords. Several user studies were performed to test the security and memorability of the passwords which users created with this scheme.

The results of these studies and general discussion are presented in the Chapter 8.

1.7 THESIS ORGANIZATION

The thesis has two main parts. The first part focuses on traditional text-based passwords: it investigates the usability and security problems caused by user behaviour in text-based password authentication domain. Some empirical studies are described, which aim at finding usable solutions to motivate users to create strong and memorable passwords as well as persuading them to avoid undesirable password practices in organisations. The second part of the thesis investigates alternative password mechanisms to text-based passwords and mainly focuses on graphical passwords. After a review of the existing graphical password mechanisms, it introduces a novel hybrid password authentication scheme including text and graphical passwords.

The thesis consists of eight chapters, broadly presenting background and related work, and analysing and discussing the findings of the empirical studies conducted to find usable solutions to password security problem.

Following this introduction chapter, Chapter 2 presents the background information and potential security issues of knowledge based authentication mechanisms focusing on text passwords. It describes the human factors that play an important role in the password authentication, and discusses the significance of balancing security and usability issues in password authentication systems. This chapter also lists possible security attacks and countermeasures in password authentication and presents a broad review of previous works related to password security.

Chapter 3 reviews the related behaviour change theories and persuasion strategies. Several selected appropriate persuasion approaches presented in this chapter will be utilised and evaluated in the following chapter.

Chapter 4 suggests the idea of utilising appropriate persuasion approaches to make users behave in a desired manner about password security. Although most organisations are aware of the importance of computer security, they have difficulties with teaching and influencing their users to behave securely. Existing studies on new instructions and security measures are still not enough to encourage users to avoid insecure password practices. Psychologists and other social scientists have suggested some methods and approaches for effective behavioural change which are discussed in the previous chapter in detail. This chapter includes some empirical studies which were conducted with employees of some big organisations using the aforementioned behavioural change methods and discusses whether using persuasive behavioural change methods can make users behave in a secure manner thus providing better password security in organisations.

Since the results of the empirical study presented in Chapter 4, and some previous research proved that the traditional methods of imposing excessive restrictions have not been very successful, it is suggested that a system that subtly persuades users and offers concrete advice may be more successful. Thus, based on the information gathered from previous studies and cases, Chapter 5 explores whether motivating users with an effective password advice and useful instructions to create strong and memorable passwords is better than obliging users to apply strict password policy rules. This chapter provides a broad understanding of human factors-caused security problems and offers a reliable solution by encouraging users to create their own formula to compose passwords.

Chapter 6 is a background chapter for the second part of this thesis, and presents a broad review of the existing authentication mechanisms. It emphasises the strong and weak sides of each mechanism, to find out whether a good alternative to traditional passwords exists considering certain criteria such as affordability, compatibility and ease of use. After analysing all the alternatives, it concludes that text-based passwords remain the most preferred mechanism followed by graphical passwords. Since text-based passwords are still the most prevalent method and graphical passwords are the most promising alternative, this chapter also discusses some solutions to improve security and usability of these passwords.

In Chapter 7, a new password authentication scheme based on text and image is introduced. It suggests using an integrated authentication mechanism, and questions

whether the vulnerabilities of the text and graphical passwords are decreased thus resulting in an improved security level with this scheme. A web application has been designed to allow participants to test the hybrid scheme's effectiveness.

Finally, Chapter 8 presents an overall discussion and conclusions drawn from the thesis. It describes the further studies which could be done to extend the research question examined in this thesis.

CHAPTER 2

BACKGROUND

2.1 INTRODUCTION

This thesis focuses on both forms of knowledge-based authentication (KBA): text-based passwords and graphical passwords. KBA can be defined as a human entity providing some secret information which was previously shared with the system to authenticate itself (Cranor and Garfinkel, 2005). Users are expected to remember the shared secret to be able to authenticate themselves but it does not matter if they apply coping strategies such as writing down the secret information to remember it.

Other authentication mechanisms based on who the user is –biometrics- (Jain, Ross and Pankanti, 2006) and what the user has – token based authentication systems- (O'Gorman, 2003) do not require any secret knowledge to be remembered. Biometric systems use the biological and behavioural characteristics of user, such as fingerprint, iris or keystroke to identify and authenticate themselves. Token-based authentication systems require users to have and use an item, such as smart card or mobile phone. Key-based authentication systems, such as Kerberos (Neuman et al., 2005) and PGP (Callas et al., 2007) typically work on secret keys which are supposed to be stored by a machine. Figure 2.1 illustrates the most common user authentication methods.

Knowledge based authentication is popular because it is relatively cheap to implement and typically does not require any additional hardware. In theory, KBA schemes are considered to be very secure, but in practice its security is not often adequate because of the lack of uniqueness and complexity of the shared secrets that users can remember. There has been proposed various forms of KBA schemes by researchers. In this chapter, we will primarily focus on the most common form of KBA which is text password. Next sections will review the literature on related usability and security issues of text passwords which emanate from use and research in the field, including password attacks and proposed solutions to text password problems.

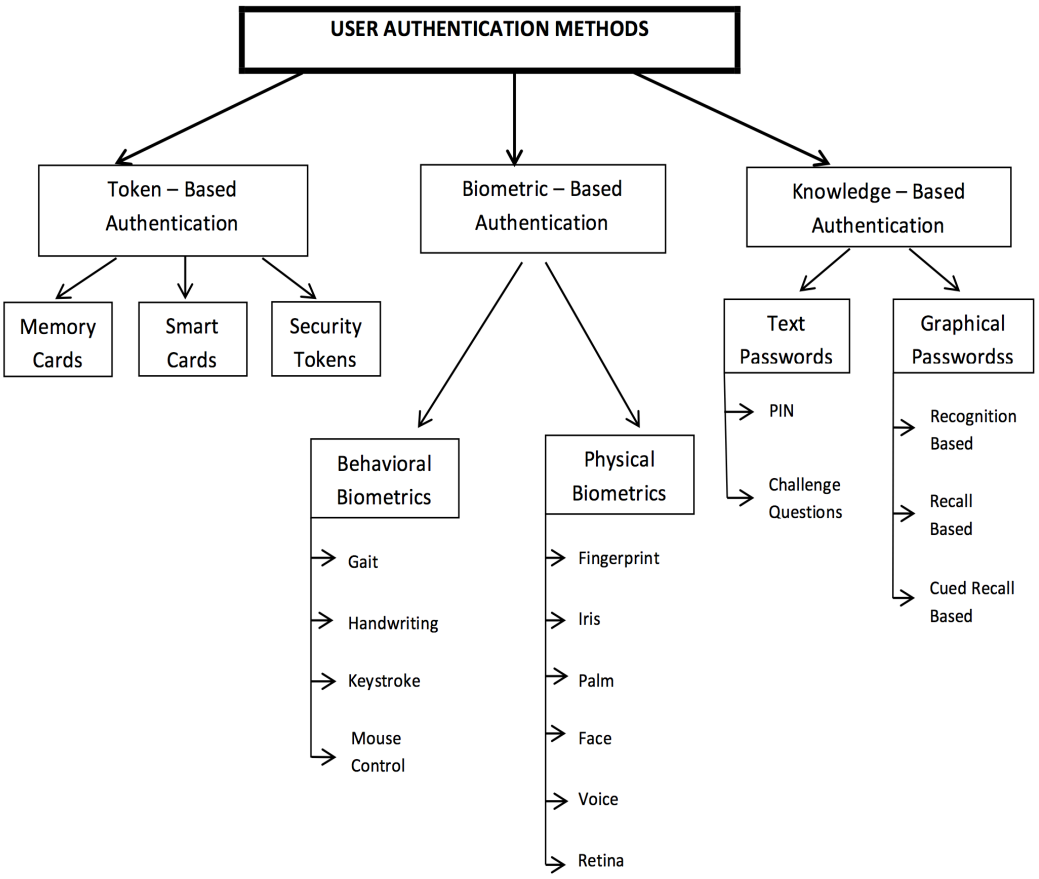


Figure 2. 1 User Authentication Methods

This thesis focuses on the usability and security issues of text and graphical password schemes. Regarding security, there are various kind of attacks to passwords, including brute force attack, social engineering, phishing and more. Within the scope of this thesis solutions to defend against password guessing attacks and shoulder surfing attacks will be specifically examined while maintaining security against other attacks. We will not take into consideration the additional mechanisms which can deter or prevent password guessing. We believe usability and security provided by these mechanisms which is in addition to the security of the main authentication scheme should be evaluated separately.

2.2 KNOWLEDGE BASED AUTHENTICATION

From the beginning of computing, knowledge-based authentication (KBA) has been the most commonly used technique to provide users accessing to computer systems securely. It seems it will remain predominant for more years to come. Despite KBA schemes' popularity, they have many known usability problems which have not yet been entirely solved. According to a study, a user has on average 25 online password-required accounts and uses eight passwords per day (Florencio and Herley, 2007). As users are expected to use different passwords for each account to avoid security failures, it is difficult for the brain to remember many discrete sets of illogical and random bits of information and then associate each set with which account. The user's response to this situation is generally adopting strategies such as choosing weak passwords or writing them down, which ultimately undermine the security of the systems they use (Klein, 1990). Some methods are used to replace this subversive behaviour with appropriately suitable behaviour for authentication (Wood, Bruner and Ross, 1976). These methods aim to direct user behaviour by implementing strict password creation guidelines (Inglesant and Sasse, 2010), proactive password checkers (Yan, 2001) or password expiry (Zhang, Monrose, Reiter, 2010), to ensure a high security level. However, recent research shows that these advices, measures or system features don't always work as expected. They sometimes have negative effects upon usability and security, contrary to designers' intentions. Where users are forced unreasonable constraints, they may more likely adopt insecure workarounds which are easy to use for them (Proctor et al., 2002). As it is well known, users mostly don't follow the strict security guidelines prescribed within KBA schemes (Zviran and Haga, 1993). Both system administrators and end-users struggle with the scenario where it is difficult to balance the security and usability of the authentication system. Although compromising one of them leads more threatening scenarios, the system needs to be sustained somehow. This shows that the current forms of KBA schemes which are unable to offer solutions to current socio-technical authentication problems, have to be abandoned in the future (Kotadia, 2004). Thus, it is inevitable to reform the existing KBA schemes.

In the recent years, security researchers have focused on designing secure and usable systems (Cranor and Garfinkel, 2005). Implications of usability studies in human computer interaction (HCI) field have revealed (Rogers, Sharp and Preece, 2011). This immature research field of *usable security* (sometimes stated as *user-centred security*)

defends including users in the design and evaluation phases of security systems. Within this context, design of graphical passwords as an alternative method of KBA aims to provide desired balance between security and usability taking cognitive limitations in human memory into consideration (Biddle, Chiasson and Von Oorschot, 2011; Suo, 2005). Cognitive theory of the picture superiority effect suggests that if a concept is presented as a picture rather than as words or numbers, it is more likely remembered (Shepard, 1967). Various graphical password schemes have emerged using the advantage of this superiority of human memory on recognizing images better then texts. Experiments and evaluations measuring memorability of these schemes have come up with promising results (Brostoff and Sasse, 2000; De Angeli et al., 2002; Wiedenbeck et al., 2005b).

Despite the advantages of graphical passwords for their usability and flexibility of computer infrastructure supporting the graphical password schemes' interfaces, graphical passwords are still rarely used. There are many reasons of this disapprobation, including cost issues and users' habits. Actually, before proposing new graphical password schemes, user behaviour issues which already causes problems in traditional password based authentication should be examined in detail. This is because issues of human perceptions and their consequential responses often cause security failures no matter which authentication schemes are used. Moreover, different authentication requirements and designs of various platforms increases the difficulty for users to adopt each of them. Sasse et al. (2001) suggest that security engineers should adopt a more holistic approach by including the context, the technology and also the user in the phases of design and evaluation of security mechanisms.

2.3 TEXT PASSWORDS

Text passwords are the most widely deployed and used authentication scheme in computer systems. However, they have known security issues such as vulnerabilities to brute-force and dictionary attacks. Therefore, organisations seek solutions to store passwords securely. Users' plaintext account passwords were stored in a file through a simple text password system which was initially developed by Unix systems (Morris and Thompson, 1979). The system has serious security issues that put users' passwords at risk of being compromised as a knowledgeable user could easily have access to the file.

Wilkes (1968) proposed to encrypt new passwords before storing them in database when the account is created. With this method, at the login phase, the password entered by the user would be first encrypted and then be compared to the previously stored encrypted-password for that user. If there is a match, the user would be granted access. Although this encryption improved the security level of the password system, it is still too risky, because, if the encryption key was broken, then all the passwords would be compromised. To eliminate this risk, Evans, Kantrowitz and Weiss (1974) proposed to apply a one-way hashing function (Lamport, 1981) to the entered password, instead of using encryption. Such a hash function must be computationally infeasible to reverse and find two different inputs which result in the same output. Also, for two identical inputs, their outputs must also be identical.

In case the file which contains hashed-passwords is compromised, the attacker will need to perform a password guessing attack to obtain the plaintext passwords. The attacker can select and hash a candidate password, and compare the result to each of the hashed password in the file. If there is a match, it means that the attacker's guess is successful so that candidate password is the actual password of the related account.

There are other techniques to store text passwords securely, such as salting and slow hash functions (Klein, 1990). These can be used not only with KBA schemes but also with other authentication mechanisms where users are granted access if they provide the right credentials that match the stored ones.

Differences between system assigned and user chosen passwords, password spaces and password restrictions and advice are important issues that should be taken into consideration during the design and evaluation of any KBA schemes. These issues are listed in the following sections.

2.3.1 Challenge Questions

Challenge questions or personal verification questions (PVQs) are another form of text passwords. When users are registering for an account, the system may ask them to answer a few challenge questions. If the user is unable to access their account through the primary authentication method later (if they forgot their text password for example), the

system will prompt the user to answer some of the challenge questions that were asked during registration. If the user's answers match their previous answers in the registration stage, then the user is directed to reset their passwords and allowed them to access their account.

The earliest versions of challenge questions are cognitive and associative passwords (Haga and Zviran, 1991; Pond et al., 2000 and Zviran and Haga, 1993). Cognitive passwords require users to answer questions about something they probably intrinsically know such as users' facts, interests, or opinions. They are easy to remember for users, but risky too, because it is highly possible that people who are close to the user can guess the password. Associative passwords were pairs of words, where the user responded to challenge words with the correct associated words (Haga and Zviran, 1991). No security analysis of either scheme was published at the time. A researcher has contributed to this area by classifying the most common types of challenge questions in a framework (Just, 2003, Just, 2004). Also, some usability and security experiments and analysis on user-chosen question and answers were performed (Just and Aspinall, 2009, Just and Aspinall, 2010). They found that although users select low-entropy questions they still have difficulty remembering the correct response. Schechter et al. (2009) found similar results in a study where users were asked to answer challenge questions taken from the four most popular webmail providers (AOL, Google, Microsoft, and Yahoo!). Challenge questions may be more insecure that originally thought, since personal information about users is becoming increasingly publicly available through social networking websites and the Internet in general (Rabkin, 2008). Thus, challenge questions may provide more assistance to password crackers than legitimate users.

2.3.2 PINs

Personal identification numbers (PINs) are a kind of text password which are composed of only digits, mostly four or five characters long. They are commonly used for the systems whose input was mainly numeric, such as telephone systems and automatic teller machines (ATMs). PINs have many security and usability problems such as small password space and memorability problems (Anderson, 1993; Clarke and Furnell, 2005).

2.4 GRAPHICAL PASSWORDS

The other form of knowledge based authentication is graphical passwords. Graphical passwords will be detailed including classification of the graphical passwords and security-usability issues in Chapter 6.

2.5 PASSWORD SECURITY

The following sections discuss several password security-related issues including password space, password creation rules and advice as well as the password attacks.

2.5.1 Password Space

The total number of different passwords that can be supported by an authentication system is called theoretical password space (TPS). Password spaces tend to grow exponentially in size, and are typically expressed in bits, which is the base-2 logarithm of the total number of possible distinct passwords. Password length and alphabet size are the main factors in computing TPS.

$P = N^L$ is the equation that expresses the relationship between P, N, and L where:

P = password space
N = number of alphabet symbols
L = password length

For example, a typical personal identification number (PIN) consisting of 4 digits using an alphabet of 10 digits (e.g., 0-9) are to be generated.
$P = 10^4$
That is, 10,000 unique 4-digit passwords could be generated.

It has a TPS of $\log_2 (10^4) \approx 13.29$ bits.

Although TPS is often used to compare the security of authentication mechanisms, it is not an accurate measure of the security of the authentication systems which is based on user-chosen passwords. This is because calculating the TPS of a password starts from the assumption that the password is constructed of completely randomly selected

characters. However, users do not select passwords randomly. They choose passwords which are meaningful to them to remember easily. The space of passwords that are likely to be actually chosen by users is called effective password space (EPS). Since users must choose a password supported by the system EPS is always a subspace of the TPS.

To improve the password security, it is important that an authentication scheme has a large EPS, that is desirably as close as possible in size to the TPS. To enlarge EPS, users should be guided to choose unpredictable passwords. Measuring an authentication system's TPS is simple but there is no definitive way to measure the EPS. Text password restriction policies are used to guide users' password selection to quantify EPS. NIST (Burr et al., 2006) is the most widely-known model to measure security. However, recent studies have proved this model's inaccuracy to measure the actual security provided by password restriction policies (Castellucia et al., 2012; Clair et al.; 2006; Komanduri et al, 2011; Weir et al., 2010). Although the most likely chosen passwords can be used to measure the EPS, this measure would not be very accurate as it depends on how the most likely chosen passwords are determined.

Other related studies to EPS which examine the content of users' passwords do not directly indicate the general user behaviour. While lab studies (Vu et al., 2007) generally do not give generalizable results as they lack the ecological validity, field studies (Florencio and Herley, 2007; Weir et al., 2010) usually concern with specific type of systems protected by passwords (e.g. users' different password choices for bank account and ordinary websites). There should be more studies to be conducted to produce more generalizable results.

Florencio and Herley, in their later study (2010) revealed that popular websites which are likely targets for attacks chose the least restrictive password policies that requires users to create passwords of only 20 bits. This is probably the largest text password EPS that users can tolerate.

2.5.2. Password Creation Policies

Password restriction policies are a series of rules which determine the content and format of the passwords accepted by an authentication system. These policies are used by

system administrators to enhance computer security by guiding users to create more secure passwords.

Firstly, Morris and Thompson (1979) proposed a password system that imposed password restrictions, with the aim of helping users choose more secure passwords. They suggested that if passwords consisting of single-case characters should be at least 6-characters long otherwise 5-characters long.

A standard for *password usage* was published by the Federal Information Processing Standards (FIPS) in 1985 (Federal Information Processing Standards (FIPS) 1985). It has many suggestions for end-users and security system administrators about content and general use of passwords. However, Sasse et al. (2001) suggested that password policies should not be based on these guidelines, as the computing environment and capabilities have changed considerably since 1985. The FIPS password usage guidelines were withdrawn in February of 2005 without being replaced or updated. In 2006, the National Institute of Standards and Technology (NIST) updated the "Electronic Authentication Guideline" (Burr et al., 2006) to be used by security system administrators for the implementation of electronic authentication. This guideline provides heuristics to measure the strength and efficiency of a password restriction policy considering bits of entropy to determine a password value's uncertainty. In this guideline, Estimation of Shannon's Entropy (Shannon, 1951) was used for the entropy calculation. However, several studies (Castellucia et al., 2012; Komanduri et al., 2011; Clair et al., 2006; Weir et al., 2010) have found that passwords created with particular password policies were more difficult to guess than the ones created with NIST model suggestions.

Komanduri et al. (2011) conducted a large web study to compare four different password restriction policies. They found that users have less difficulty to comply with creating a 16-character minimum password compared to an 8-character minimum excluding dictionary words or further restrictions. Beside the passwords at least 16-character long provide the best security. They also measured the password strength using a calculation entropy (Shay et al., 2010) thus they showed some misconceptions about how restriction policies affect password strength. Their findings conclude that adding digits much increased the entropy of passwords, but excluding dictionary words increased the entropy less than expected. Also, the findings showed that passwords created by users

barely exceeded the minimum requirements.

With another form of password restriction policy commonly known as *proactive password checking*, the system itself performs a dictionary guessing attack on the user's password like an attacker during registration or reset. The researchers recommended the disallowance of some passwords which include dictionary words (and similar derivatives), repeated characters ("aaaaa") and common keyboard patterns ("qwerty"). They also suggested that digits-only passwords should not be allowed by the system (Klein, 1990; Klein and Bishop, 1995). Similarly, Schechter et al. (2010), suggested that the authentication system should reject statistically the most frequent passwords chosen by system users.

Contrary to what is believed, some researchers have claimed that password restriction policies do not improve password security (Adams and Sasse, 1999). There has been some lab (Vu et al., 2007) and field studies (Keith et al., 2007) conducted to test this claim. Results show that it is difficult to create and remember passwords for users when they are enforced to employ strict and complex password policies. To cope with remembering difficult passwords, users commonly adopt insecure password practices. These policies also help attackers to guess passwords more efficiently as they can decrease the number of candidate passwords based on the restriction policy. In their website study Florencio and Herley (2010) found that users only tolerate the restriction policies if they have no other choice. However, most of the systems use policies requiring passwords 20-bits strong. This causes a burden on users to deal with a cumbersome password restriction policy. The authors also note that websites which typically users do not care too much to create strong passwords to log in are often the most popular ones and also the most likely to be attacked as they have great amounts of assets for hackers. If such popular websites continue to force strict password policies, it might increase the security slightly in exchange for a considerable usability cost.

2.5.3 Password Creation Advice

Most systems that impose password restrictions offer their users password advice about creating passwords. The purpose of password advice is both making adoption of password policy rules easier and motivating users to create stronger passwords. In a study,

password practices of ten popular internet sites which enforce password policy rules and offer password advice was examined (Furnell, 2007). That the websites' password restriction policies and password advice are vastly different sometimes caused conflict between them. In most of the websites, password advice was found ambiguous and unhelpful by users. As existing password policies and advice are far from being consistent and effective, it is not easy for users to form accurate mental models of how to create a secure and memorable password.

2.5.3.1 Mnemonic Passwords:

There is a wealth of research investigating the best way to advise users to create secure and memorable passwords. In an attempt to encourage users to create easy to remember passwords mnemonic phrase-based passwords have been first proposed by Barton and Barton (1984). Mnemonic passwords are derived from a memorable sentence where users generally use a letter of each word in the sentence. Although most of the password advice research is about mnemonic passwords they are rarely recommended to use in practice (Furnell, 2007).

The first and largest experiment on mnemonic passwords is published by Yan et al. (2004). They conducted a field study with 288 student participants to compare mnemonic passwords along with a password advice and random passwords. The password advice was that the password should be at least seven characters long and contain at least one different character than a letter. After a month, they successfully cracked the 32%, 8%, and 6% of the control, random, and mnemonic groups' passwords respectively. All the cracked mnemonic and random passwords contained dictionary words despite the password advice provided to users suggest not to use them. Only users who created mnemonic password used special characters, probably because the examples provided to them contained special characters. Therefore, the authors stated that password advice should definitely convince users to use special characters in their passwords although 10% of users did not comply with the advice. By measuring password memorability, the authors also found that mnemonic passwords were at least as memorable as typical passwords but much more secure than them, and they are at least as secure as random passwords but much more memorable than them.

However, Kuo et al. (2006) later showed that mnemonic passwords may not be really secure as thought. They conducted a study with 290 participants asking half of them to create a mnemonic password. They used John the Ripper (Openwall.com, n.d.) with a custom dictionary of 400,000 candidate mnemonic passwords from popular sources to test the security of the passwords. They managed to crack 4% of mnemonic passwords. The authors asked the other half of the participants to create standard passwords and cracked 11% of them with a 1,200,000 entry standard dictionary. The authors conclude that mnemonic passwords were not more secure than regular passwords, because users commonly use phrases which are easily found on the Internet to create their passwords. Besides, a higher percentage of passwords can likely be cracked by building a larger mnemonic dictionary by an attacker.

There are more studies which present the different ways to generate a mnemonic password. Vu et al. (2007) used two mnemonic password generation methods in a user study and let all users choose their own sentence. In the first group, participants were told to use the first letter of every word in their sentence, and in the second group, participants were instructed to transform their chosen sentence into a mnemonic string of characters. For example, they would transform the "I had four snakes" sentence to "EyeH@4$nake$". As the passwords created with the mnemonic string method typically have more characters, they were thought more secure. However, the authors found little difference in password creation times, login times, and recall error rates between two methods. In a previous study, they had also found that passwords which contain more characters were more resistant to cracking (Proctor et al., 2002). Unfortunately, as the way of substitute words and characters suggested in the study (Leet, 2016) are well known by attackers, mnemonic string method may not be very much secure as previously thought.

2.5.3.2 Password Chunking:

Very little research has been done in password advice apart from mnemonic passwords. There are studies on the use of chunking (Miller, 1956 and Cowan, 2001) to help users to create easy-to-remember passwords. Carstens et al. (2006) performed a field study applying chunking theory to an organisational password guideline. They compared common password advice (that the password should contain at least 7 characters, be a combination of symbols and letters, not contain repeated characters more than twice, not

be a dictionary word or personal data), to two-chunk, three-chunk, and four-chunk passwords. The authors found that four-chunk passwords were not only longer but also more memorable than the 7-character, two-chunk, or three-chunk passwords. However, they did not carry out a security analysis of the created passwords, or the password advice itself. Therefore, in fact four-chunk passwords may have been less secure, as they contained fewer distinct symbols than other passwords. Further- more, since participants were explicitly told what to use for their chunks such as participants' first and last initials, spouse's initials, employment start date in the password guideline, it would not have been difficult to predict participants' passwords for an attacker, particularly one familiar with the user.

2.5.3.3 Password Strength Meters:

Password advice can also be represented with a tool measuring strength of the password and giving users a numerical result or statements such as 'weak', 'strong', 'very strong'. These tools are called "password strength meters" which typically illustrate the strength of the currently chosen password when a user is registering for an account. The meters are commonly used by popular websites (Gmail, PayPal and eBay). In an online user study conducted with over 2000 participants, different password strength meters were evaluated (Ur et al, 2012). The results showed that the passwords created by users who used password meter were more difficult to guess than the passwords created by users who did not use a strength meter. Furthermore, users created much stronger passwords when they used stringent password meters. However, the authors found that meters which are too stringent may cause users to lose motivation and ignore the meter. In another study, a novel method called Adaptive Password Strength Meters (APSMs) were proposed to measure password strength (Castelluccia et al., 2012). Adaptive Password Strength Meters use Markov models (Manning and Schutze, 1999) to measure a password's strength as the collective probability of each character following the previous characters in the password. These probabilities can be calculated either based on a training set of passwords or the passwords currently in use. Although the authors claim that APSMs is better than any other proposed password strength metric to date as it can score passwords closer to the "ideal" password strength meter, there has not been conducted any formal usability study of APSMs and a practical security evaluation.

Kelley et al. (2012) introduced different calculators for estimating the number of guesses required to crack a password using a particular cracking algorithm. They calculated the percentage of passwords which can be cracked with the implemented algorithm given a number of guesses. To compare cracking performance across algorithms, guess number calculators for several cracking algorithms on the same set of passwords can be implemented. Guess number calculators may be considered the more practical and efficient method of proactive password checking (Bishop and Klein, 1995) than running a computationally-intensive password cracking algorithm (Forget, 2012).

2.5.4 Password Attacks

Brute Force Attack:

This attack involves running through the combinations of potential passwords to find on the correct one. Attackers usually start trying the most common passwords (“password”, “123456”, “qwerty”) as well as the combinations of account holder’s personal information (name, birthday etc.) if they are known. Then they progress trying all the possibilities through mixtures of numbers, letters, and other keyboard characters. There are scripts and applications for hackers, written specifically for this purpose which can be found on internet (Finjan Blog, 2016).

The theoretical password space of text based passwords is 94^N, where N is the length of password and 94 is the total number of alphabetical characters, numbers and the special keyboard characters. Text passwords are more vulnerable to these attacks than graphical passwords since it is difficult to track every movement of the mouse or input device (Bhanushali et al., 2015).

Dictionary Attack:

This is word-based brute force attack, in which attackers use a list of words dictionary to break the password. The dictionary includes the most likely chosen passwords by the users. If the hacker gains access to user data, it may be supplemented with existing usernames, birthdays, addresses, names of family members and so on. The difference with the brute force attack is that this attack uses a systematic key search to crack passwords. The key takes into consideration only the possibilities which are most

likely to succeed. Dictionary attack cannot guarantee to find the correct password as brute force attack eventually does.

Key Logger Attack:

In this type of attack, specific software is installed on the user's computer recording the strokes on a keyboard, clicks and movements of a mouse or even captured screenshots to a log file. These log file is used to obtain sensitive data like passwords and usernames (Finjan Blog, 2016). The possibility of success of this attack is more with the textual passwords since movements and mouse input can change in many graphical password scheme.

Shoulder Surfing Attack:

This is an observation attack where attacker can obtain the password by simply looking over the person's shoulder. This attack is more likely to succeed in crowded areas where people are not aware of the people looking at their screen and in the queues of ATMs. Most graphical passwords are susceptible to these attacks since it is easier to follow movements or clicks on an image rather than a series of keyboard characters.

Social Engineering Attack:

Social Engineering refers to manipulating people to reveal their confidential information. Attackers perform various tricks to exploit people. For example, they can call people, act as an authorized person and tell people that they need their password to resolve a network issue at people's workplace (Finjan Blog, 2016).

Phishing Attack:

Phishing attack is a form of social engineering that often uses email, malicious websites or several other channels to solicit personal information from users by posing as a trustworthy connection (Lord, 2017). The goal of a phishing attempt is to trick users to provide login credentials or other sensitive information. For example, user might be sent a phishing email by attackers appearing to come from a bank telling the user that they should reset their password for a security reason, and direct users to a fraudulent website where they can collect user's login information.

2.6 USABILITY OF PASSWORD SECURITY

Passwords authentication mechanisms mostly involve a trade-off between security and usability. The main reason of the imbalance between them is memorability problem. When users are forced to create long, complex and randomly generated passwords they are likely to write them down or forget them. On the other hand, when users choose the weak and predictable passwords they are susceptible to attacks. The researchers who tried to crack passwords conducted several experiments and the results proved the weaknesses of the user chosen passwords (Klein, 1990; Garrison, 2008). It seems more secure password means the less usable password or vice versa (Burnett and Kleiman, 2006). Some authors investigated the relationship between password security and usability by conducting several studies (Hub, Capek and Myskova, 2011).

User interface is another aspect of usability, which should be designed to provide effectiveness, efficiency and user satisfaction in a specified context of use. Usability consists of several criteria including learnability, efficiency, memorability, errors and satisfaction, and be examined in different types of user interface (Cerna and Poulova, 2009)

In relation to this study, the next section discusses the *memorability* criteria of usability causing the security-usability contradiction.

2.6.1 Memorability

Memorability is the most important issue in knowledge based authentication systems considering the limitation of human memory that puts systems security into high risk. Many studies pointed out the users' difficulty in remembering passwords. Florencio and Herley (2007) predicted that each user has on average 25 accounts which should be protected with different and complex passwords. This is mostly a difficult requirement for users (Adams and Sasse, 1999). Thus, users typically adopt coping strategies to avoid forgetting and resetting passwords.

Vu et al. (2007) tested the memorability of text passwords which are created obeying various password policy rules. They found that remembering five passwords is more difficult than remembering three passwords. Also, users tend to create passwords

which are obviously connected to the accounts, as a memory assistance coping strategy.

Chiasson et al. (2009b) conducted a study to compare the memorability of multiple text passwords and multiple PassPoints graphical passwords. They found that after the passwords were created, graphical passwords were much more easily remembered than text passwords. As remembering different passwords across accounts is challenging for users, they commonly use coping strategies to overcome the memorability issue. One of these strategies is choosing similar passwords across accounts which causes multiple password interference. This issue has been studied in a few other graphical passwords related research papers (Chiasson et al., 2007; Everitt et al., 2009; Mancur and Leplatre, 2007).

2.6.2 System-Assigned and User Chosen Passwords

In text and graphical password authentication mechanisms, either users are allowed to set their own passwords or they are assigned a typically random password by the system itself. Generally, system-generated passwords are much more secure than user chosen passwords, since users mostly choose weak or predictable passwords to remember easily. Also, most users are not aware of the probability of guessing attacks and capabilities of attackers to compromise passwords (Adams and Sasse, 1999). However, passwords assigned by the system are harder for users to memorize and remember as they generally consist of combinations of unrelated characters (Yan et al., 2004). Therefore, users would not have the chance to use cognitive methods which help memorability in creating passwords. Also, passwords that have no meaning for users consequently make them harder to remember (Vu et al., 2007; Zviran and Haga, 1993). A research study proved that memorability of system-assigned passwords and system-assigned passphrases are equivalent regarding password strength (Shay et al., 2011). This means that remembering system-assigned passwords is a great burden on human memory without any memory aid provided by the authentication system. There are other methods which have been researched to aid text password memory such as using semantic content (Jeyaraman and Topkara, 2005; Topkara et al., 2007) and cueing. However, Wright et al. (2012) found that recognition passphrases which are entered by users by selecting the assigned words from a list are not more memorable than system-assigned passwords. This

proves that some forms of memory assistance are not sufficient, so further studies are needed to evaluate effective forms of memory aid.

2.6.3 Coping Strategies

Because of the limitation of human memory users tend to adopt coping strategies to remember their passwords (Adams and Sasse, 1999). Since it is not reasonable to expect users to remember different and complex text passwords across many accounts, these strategies are in use for many years (Gaw and Felten, 2006; Inglesand and Sasse, 2010). Stobert (2014) conducted a series of interviews to investigate how users cope with the many accounts and passwords, and found that users develop rational personal strategies including password reuse and writing passwords down.

The coping strategies for passwords are as follows:

Writing Passwords Down:

When users are required to follow strict password creation policies or to change their password frequently, they are likely to resort to writing their passwords down to overcome the memorability issues. Results of several experiments showed that most users tend to write down their passwords except those who were given less stringent password creation rules to follow which allow users to create more memorable passwords (Adams and Sasse, 1999; Inglesant and Sasse, 2010).

Although writing passwords down is usually considered to be insecure, some security researchers defend writing passwords down if they are kept somewhere safe (Cheswick, 2012).

Password Reuse:

An alternative strategy to handle passwords is using the same or very similar passwords across multiple accounts. Previous research showed that password reuse strategy is widely employed by users (Chiasson et al., 2009a; Florencio and Herley, 2007; Stone-Gross et al., 2009). However, it has security risks since it increases the chance of obtaining passwords for attackers. Attackers could discover the reused password through a leaked password set and they can access several accounts (Das et al., 2014; Florencio and Herley, 2007; Gaw and Felten, 2006; Hayashi and Hong, 2011; Stobert, 2014).

Password Sharing:

According to common password policy applied in organisations, each account which might contain confidential information should be controlled by an individual. However, this model can fail in organisations when teamwork is performed. Users generally share their passwords to work on same thing (Adams and Sasse, 1999). Patrick (2008) found that users' share corporate and external accounts and password-protected documents although, security policy of their organisation do not allow them to do so.

According to Singh et al. (2007), password or PIN sharing can be acceptable in some cases as it becomes necessary.

Weak Password Selection:

As is evident by many research, users tend to select predictable passwords (Florencio and Herley, 2007; Inglesant and Sasse, 2010; Morris and Thompson, 1979; Weir et al., 2010) because of the memorability issue. According to Florencio, Herley and Coskun, (2007) when users perceive the low risk of threats or they do not care much the account protected by the password, they are more likely to choose memorable password instead secure ones (e.g. complex, long and meaningless passwords). This may be caused of users' misunderstanding of actual threats or attackers' capabilities (Gaw and Felten, 2006). Some researchers argue that the solution to coping strategies for passwords could be informing users about threats (Herley, Van Oorschot and Patrick, 2009; Whitten and Tygar, 1999)

2.6.4 Password Managers

Another approach to memorability problem is password managers, which store passwords and enter them automatically to the associated accounts. Browser-based password managers save passwords for a specific website and automatically input them when the website is revisited. Dedicated password managers either generate a password at login phase by hashing the user's master password with the website information, or they keep the user's passwords in a password wallet which is protected by a master password (Chiasson, Van Oorschot and Biddle, 2006). In either way, users have to use a master password. In case the master password is hacked, the attacker can gain access to

user's all accounts.

2.7 SUMMARY

This chapter has presented the background information to understand the research presented in this thesis. It has pointed out the security and usability issues of password authentication mainly focusing on text passwords. Since strong passwords are not memorable, and easy to remember ones are also easy to creak, many possible solutions have been offered by researchers so far. However, none of them seems to solve the problem completely because most of them put their focuses on technical issues rather than human factors.

To align security and usability in password authentication, human factors problem should be investigated which is the main focus of this thesis. Proposing usable solutions to password problem will likely motivate users to behave in security-conscious way thus improve the password security.

To increase the users' motivation to adopt good password behaviour and abandon the bad ones some behaviour change theories and persuasion strategies can be used. In the next chapter, several related psychological behaviour change theories and persuasion approaches will be reviewed.

CHAPTER 3

REVIEW OF RELATED BEHAVIOUR CHANGE THEORIES AND PERSUASION STRATEGIES

3.1 INTRODUCTION

There are several psychological behaviour change theories such as theory of planned behaviour and protection motivation theory to be used to change employees' insecure password related behaviours in organisations. In addition to these methods, in recent years, persuasion approaches have been commonly used to motivate employees to behave in a secure manner.

Following sections reviews the related behaviour change theories such as the theory of reasoned action, the theory of planned behaviour and protection motivation theory in general, and several persuasion strategies. Then several appropriate persuasion approaches to change unwanted password behaviours in organisations will be examined.

3.2 THEORETICAL BACKGROUND

In order to achieve changing behaviour, firstly attitudes and intentions have to be changed. The related psychological behaviour change theories are presented below.

3.2.1 Theory of Reasoned Action

Theory of reasoned action by Fishbain and Ajzen (1975) states that the psychological requirements of intended behaviour are attitudes and perceived social norms. It assumes that people rationally calculate the costs and benefits of a certain action before engaging, and think how important others will see behaviours that need to be taken into consideration (Zakaria, 2013).

The theory's components are as follow (Figure 3.1):

- *Attitude towards the behaviour*: the person's consideration whether the behaviour is good or bad
- *Subjective norm:* perceived social pressures by person to perform the particular

behaviour

. *Behavioural intention:* the intent or plan to perform the behaviour

. *Behaviour:* the action itself in a particular situation

The theory supports that changes in behaviour and normative beliefs of an individual will eventually affect the actual behaviour.

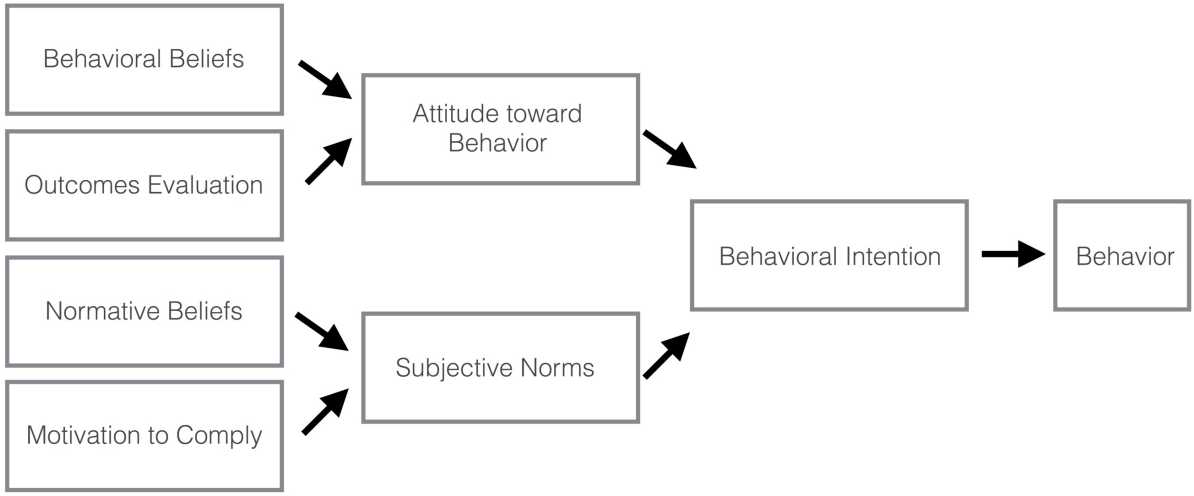


Figure 3. 1 Theory of Reasoned Action (Fishbain and Ajzen, 1975)

According to the framework offered by the theory, behaviour can be predicted from attitudes and norms (Fishbein and Ajzen, 1975) Several researchers who tested these proposals have found that attitudes and subjective norms estimate intentions thus predict behaviour (Hale, Householder and Greene, 2002; Sutton, 1998).

One of the limitations of this theory is its assumption that people have control over their behaviour which is not always possible (Fazio, Powell, Williams, 1989). If people fail to perform their intention, they do not act on attitude or norm. Ajzen attempted to fix this problem, by proposing an alternative approach known as the Theory of Planned Behaviour (Ajzen, 1991).

3.2.2 Theory of Planned Behaviour

The theory of planned behaviour (TPB) developed by Ajzen (1988) is designed to

explain and predict human behaviours in a particular context. In fact, it is a social psychology theory, it has been widely used to explain the behaviour of many different disciplines. According to this theory, the intention is the primary explanation of individuals to carry out an act; and the intentions are influenced by *attitudes toward the behaviour*, perceived social pressure or *subjective norms* and *perceived behavioural control*. In the theory of planned behaviour there are three basic factors that influence the underlying intentions of one's behaviour. These are: behavioural attitudes, perceived social pressure and behavioural control, or, in other words, perception of self-efficacy (Fishbain and Ajzen, 1975). Figure 3.2 illustrates the components of the theory of planned behaviour (Ajzen, 1991).

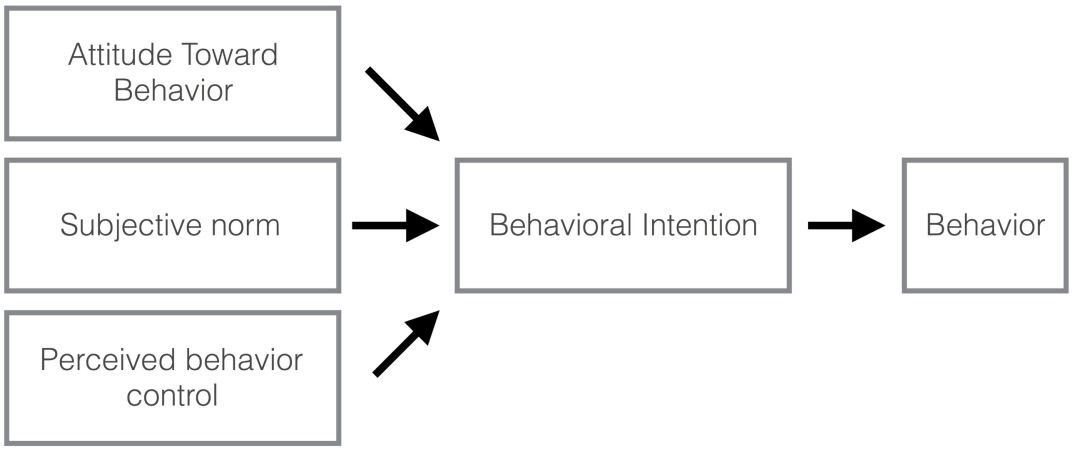


Figure 3. 2 Theory of planned behaviour (Ajzen, 1991)

The TPB claims that behavioural achievement can be provided by intention and behavioural control. It is comprised of six constructs which are attitudes, behavioural intention, subjective norms, social norms, perceived power and perceived behavioural control that collectively represent a person's actual control over the behaviour (Bada and Sasse, 2014). As an additional component to the theory of reasoned action, perceived behavioural control, indicates the people’s perception of how much control they have over the behaviour.

3.2.3 Protection Motivation Theory

Protection motivation theory (PMT) was originally developed as a framework to explain the influence of fear appeal on attitudes and health behaviour (Rogers, 1975). The theory suggests that if the threat can be perceived by people as fearful, they will more likely act in a cautious manner, and try to prevent the possible threat (Humaidi and Balakrishnan, 2012).

The theory has been later extended (Rogers, 1983) to provide more explanation of the impact of persuasive communications focusing on the cognitive processes which mediate behaviour change. PMT is organized around two cognitive processes: the process of threat appraisal and the process of coping appraisal. The following three threat appraisal factors explain how threats are perceived by people.

Vulnerability: Perception that the individual is sensitive to the threats.

Perceived severity: the importance of the threat.

Rewards/benefits: motivation for increasing or protecting the undesired behaviours.

In addition to threat appraisals, PMT also includes three coping appraisal factors that explain an individual's ability to handle the threat. These coping appraisal factors are as follows:

Response efficacy: beliefs as to whether the recommended action step will actually avoid the threat.

Self-efficacy: the extent of the belief in implementing the protective behaviour.

Response cost: removing reinforcement for an undesirable or disruptive behaviour.

Figure 3.3 illustrates the PMT framework and its components.

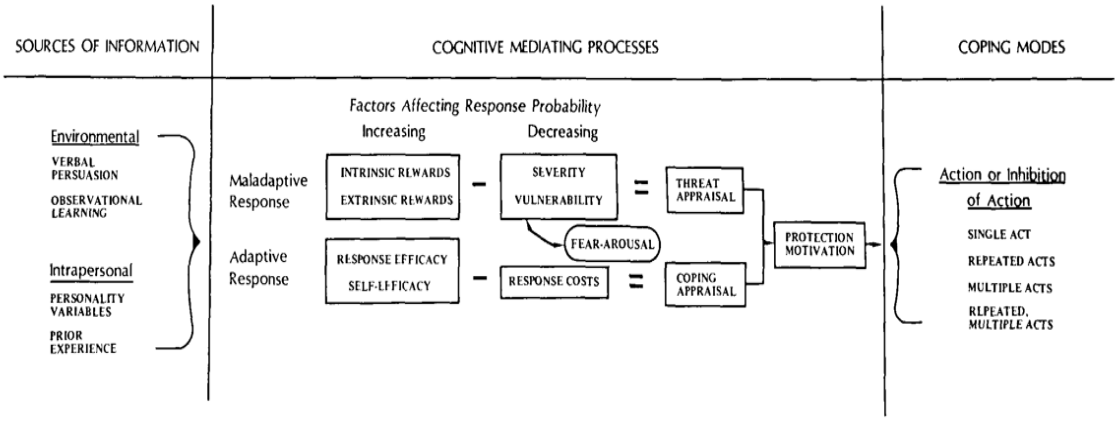


Figure 3. 3 Protection Motivation Theory (Ajzen, 1991)

Due to its wide scope of applicability, protection motivation theory has been applied by many researchers from different disciplines. In recent years, many security researchers especially those focusing on information security behaviour (Herath and Rao, 2009; Johnston and Warkentin, 2010; Pahnila, Siponen, Mahmood, 2007; Srisawang, Thongmak and Ngarmyarn, 2015) and user motivation (Posey et al., 2011; Posey, Roberts and Lowry, 2015) studied this theory.

The studies applied PMT in the information security field mostly focused on vulnerability, severity, users' habits and prior knowledge as these are more relevant to the outcome of information security policy compliance (Herath and Rao, 2009; Vance, Siponen and Pahnila, 2009; Zhang and McDowell, 2009).

Fear, one of the elements in PMT construct, has been also studied quite frequently. For example, Weirich and Sasse (2002) proposed the use of fear appeal in order to motivate users to comply with the secure password behaviour. They suggested changes in the existing password guidelines by including the punishment regime enforced by organisations to inspect any misbehaviour. Some researchers proposed threats as the fear elements to turn users' attention to security compliance behaviour (Xu, Rosson and Carroll, 2007). However, the effect of fear elements especially the punishment regime is still being investigated since it may differ considering the other factors which influence employees' password-related behaviour.

The next sections investigate the persuasion elements, approaches and practices

in detail.

3.3 PERSUASION

Persuasion, which is a form of attempted influence (Cialdini, 2001), aims to change a person's beliefs, attitudes, intensions, motivations or behaviours toward some idea or another person (Gass and Seiter, 2015).

Today**,** persuasion is mostly considered as science rather than art. It is used by numerous different organisations from advertising agencies, public relations firms, marketing and sale companies as well as social activists and speech writers. This shows that persuasion is a powerful tool and when applied correctly it can lead to a beneficial outcome for both communication parties.

Researchers attempt to evaluate and increase its effectiveness in controlling behaviour following a systematic procedure (Carlins and Abelson, 1970). In this thesis, persuasion is used as an approach towards improving users' behaviour in the domain of password security.

3.3.1 Definition of Persuasion

Scholars have defined persuasion in different ways. While some communication scholars define it as a "conscious attempt by one individual to change the attitudes, beliefs or behaviour of another individual or group of individuals through the transmission of some message" (Bettinghaus and Cody, 1987), another scholar's definition of persuasion is "a successful intentional effort at influencing another's mental state through communication in a circumstance in which the persuadee has some measure of freedom" (O'Keefe, 1990).

As a combination of these definitions, Perloff (2003) defined persuasion as a symbolic process where communicators try to convince others to change their attitudes or behaviour related to a particular issue via transmission of a message, allowing them to do their choice freely. Perloff's definition has five components as follows:

1- Persuasion is a symbolic process.

2- Persuasion involves an attempt to influence

3- People persuade themselves.

4- Persuasion involves the transmission of a message.

5- Persuasion requires free choice.

Coercion is another form of attempted influence, which differs from persuasion. Coercion is forcing someone to act in an involuntary manner using intimidation, threats or some forms of pressure. If people's perception is that they have no choice but to comply, the influence is viewed more as coercive (Perloff, 2008). Persuasion is more powerful and effective in a long term as it allows people to participate voluntarily in the persuasion process (Miller, 1980), however, coercion has a short-term effect on influencing people.

3.3.2 Effects of Persuasion

Persuasion is a communication process so it involves three main elements; source (human), message, and receiver (human). In the human-computer-persuasion model the source is substituted by a computer while transmitting verbal and non-verbal messages to receiver, users. The source is also called persuader and the receiver is called persuadee in the persuasion process.

Miller (1980) has proposed that communications exert three different persuasive effects: shaping, reinforcing, and changing responses.

Shaping: This means that attitudes are "shaped" by associating some patterns with a product, person, idea or situation.

Reinforcing: This means making attitudes more resistant to change. Contrary to popular opinion, many persuasive communications are not designed to convert people, but to reinforce a position they already hold.

Changing: This means changing of people's response to a specific issue. It is perhaps the

most important persuasive impact and the one that comes most frequently to mind when the persuasion is considered.

The potential effects of persuasion by Kukkonen and Harjumaa (2008) which is similar to Miller's (1980) is illustrated in Figure 3.4:

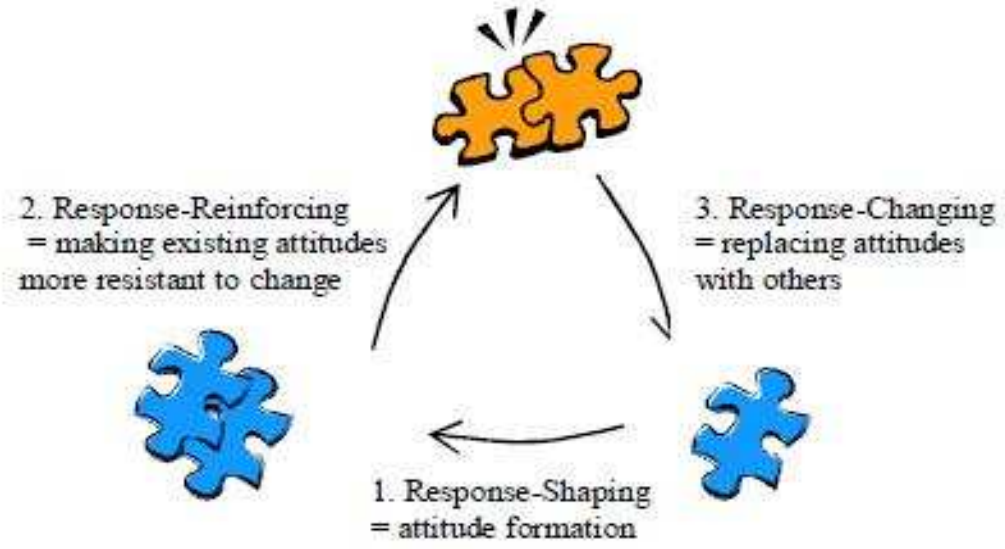


Figure 3. 4 The three possible effects of persuasion (Kukkonen and Harjumaa, 2008)

3.3.3 Persuasive Technology (PT)

Persuasive technology (PT) which has been introduced by Fogg (1998) is designed to change attitudes or behaviours of the users through persuasion. Such technologies are commonly used in many field such as sales, politics, public health and recently in human-computer interaction and information security.

PT suggests that computing technologies can motivate and influence users to behave in a desired way. Fogg (1998) categorized persuasive technologies by their functionality proposing a framework, *Functional Triad*. According to the framework, PT can function as a *tool*, *medium* and *social actor*.

As a *tool*, PT can increase people's capability to perform a target which they could not do before by making it easier for them.

As *medium*, the computer can set the format to be easily interpreted by users.

As *social actors,* PT opens the door for computers to apply social influence such as following social and dynamic rules such as greetings and apologies or animating characteristics such as voice communication or emotions (Fogg, 2002).

Figure 3.5 shows the overview of the Functional Triad focusing on principles and attributes of three functionality elements.

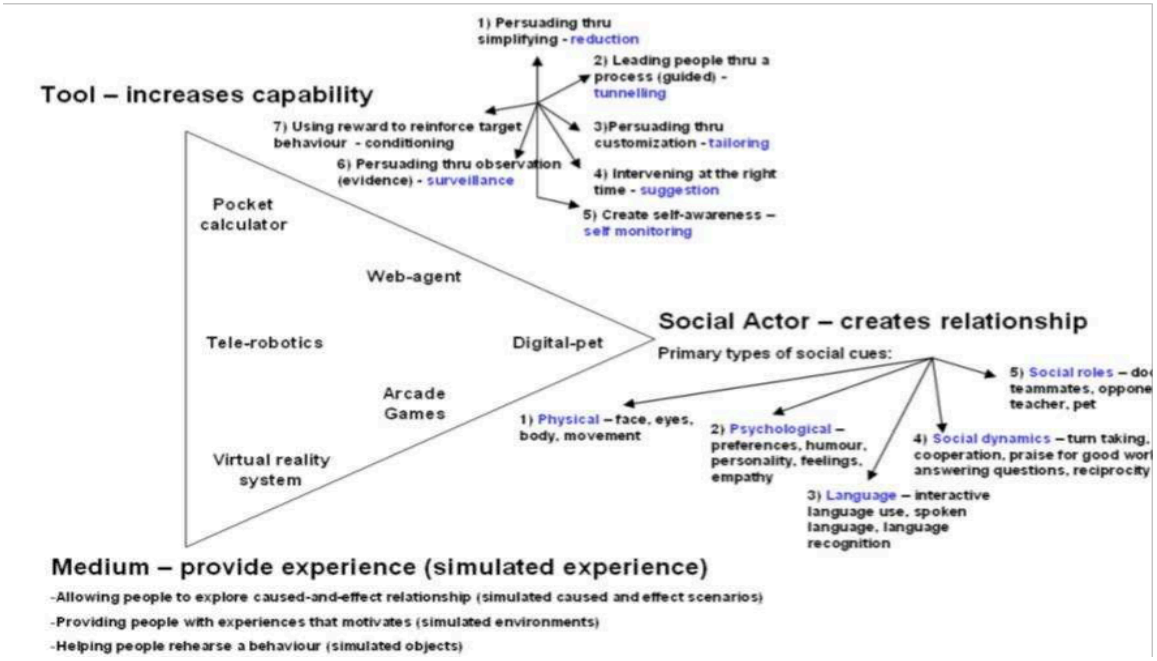


Figure 3. 5 The Persuasive Technology framework (Fogg, 1998)

In recent years, most researchers in the field of human-computer interaction have placed their focus on PT since the framework above does have its limitations and need to be improved.

3.3.4 Weapons of Influence

Weapons of influence is a persuasion method involving six principles introduced by Cialdini (1988). The principles are *reciprocation*, *commitment and consistency*, *social proof*, *liking*, *authority* and *scarcity*.

Reciprocation*:* The principles suggests that people will treat others the same way they are treated. In other words, reciprocation recognizes that people feel indebted to those who do something for them. The principle is used by charity organisations by sending gifts to potential donators. People who receive a gift are more likely to donate no

matter how the gift is. The gift does not have to be expensive or even material; information and favours can work too.

Social Proof: According to this principle, people tend to look at what other people do, before they act in a situation. Social proof has powerful effects on motivating people in different activities from charity donations to phobia remission. For example, an experiment showed that when children who are afraid of dogs see another child playing with dogs, they will be encouraged and willing to play with the dogs after a while.

Another experiment is conducted by Cialdini (2005) and his team in a hotel where visitors were provided different types of cards in their room to convince them to reuse their towels. They tested the efficiency of four types of cards on motivating hotel visitors (Polanski, n.d.).

1- The first card mentioned environmental reasons to encourage visitors to reuse their towels
2- The second card said the hotel would donate a portion laundry savings to a non-profit environmental organisation
3- The third card said the hotel had already given a donation and asked: "Will you please join us?"
4- The fourth card said the majority of guests reused their towels at least once during their stay.

At the end of the experiment, the percentage of visitors who reused their towels were per request were as sign-1: 38%, sign-2: 36%, sign-3: 46% and sign-4: 48%.

The results showed that, when guests found out that most people who stayed in the same hotel reused their towels, they were more likely to comply with the request.

Cialdini (2001) claims that the social proof principle is more powerful under two conditions; *uncertainty* and *similarity*. When people are uncertain about a course of action or if the situation ambiguous they are more likely imitate the others' decisions and actions. Also, people are more inclined to follow others who are similar to themselves (e.g. their peers, colleagues)

In the empirical study presented in the next chapter, this principle is evaluated in terms

of its efficiency on motivating employees to adopt good password behaviours. The employees are asked that if their colleagues are rewarded or punished for their insecure password practices at work, how this situation would affect their motivation to follow the password policy.

***Commitment and consistency**:* This principle suggests that people are more likely to do something after they agreed to it verbally or in a written statement. Once agreed, the person will behave consistently with that commitment.

This principle might work in situations where commitment is highly desired. Zakaria (2013) conducted a study creating a password guideline framed by this principle to find out whether users more likely comply with the password policy.

***Liking**:* According to his principle, people prefer to say 'yes' to others they know and like. People are more likely to be influenced by those who are physically attractive or similar to themselves (Burger et al., 2004). Marketers commonly apply this principle to increase the sale of their products by emphasising similarity factor that increase the overall attractiveness and likeability.

Authority: This principle states that people are more likely to listen to experts or follow the lead of experts as they respect authority. Titles or impressive clothing and even the expensive automobiles are some proven factors in lending credibility to any individual (Cialdini, 1988).

Stanley Milgram, a psychologist in Yale University, conducted several experiments in a study to show the obedience to authority. The study proved the strong pressure in society to comply with the request of a figure of authority. Many normal, educated and psychologically healthy participants in the experiments are observed to be willing to deliver dangerous and severe levels of pain to another person when asked to do so by an authoritative figure (Milgram, 1974).

In the empirical study presented in the next chapter, efficiency of this principle on motivation of employees to secure their passwords is evaluated. The employees' password practices were observed when they were given a seminar/training by a security expert who also mentions the possible threats.

***Scarcity*:** This principle relates to supply and demand. People perceive the things as more valuable and want them more when they are less available. This principle is commonly used by marketers using the limited number and deadline terms to try to convince people that the access of their products is restricted by amount and time.

3.4 SUMMARY

This chapter presented several related psychological behaviour change theories and persuasion approaches. To improve the password security and usability in organisations two persuasion strategies have been chosen to be utilised in the empirical study presented in the following chapter.

The authority and social proof principles of Cialdini's weapons of influence (Cialdini, 1988) have been selected to be used to increase users' adoption of good password-related behaviour, thus increase the information security level of organisations. To evaluate the effectiveness of these strategies in addition to reward and punishment and fear appeal strategies on employees' password-behaviours in the organisations an empirical study is conducted. The details of the empirical study are presented in the next chapter.

Next chapter will also identify several other factors including organizational, motivational and education and awareness factors affecting user behaviour, and propose some possible countermeasures to increase password security in organisations.

CHAPTER 4

IMPROVING PASSWORD SECURITY BEHAVIOURS IN ORGANISATIONS

4.1 INTRODUCTION

Today around the world, information and computing (ICT) systems are extensively used, so organisations need to keep them secure. To achieve this, they mostly develop and use information security policies that specify 'correct' behaviour of employees. Numerous researches proved that most employees do not comply with specified behaviours. While some of them are not aware of the risks or do not know the correct behaviour, most of them do not comply with the policies consciously although they know the correct behaviour.

This chapter concentrates chiefly on human and organisational factors within the information security system particularly focusing on password security. The impact of personal and organisational factors influencing employees' behaviour, irrespective of the power of technical controls can be drastic (Bishop, 2002). In this aspect, human factors-based vulnerabilities can occur because of poor security protection such as weak passwords or poor usability, and the system may become susceptible to threats. The results of useless organisational policies and insecure employee practices causes susceptibilities (Besnard and Arief, 2004).

The chapter addresses the challenges of changing employees' undesired behaviour and practices in password authentication, and proposes possible countermeasures to avoid security failures. Changing undesired behaviour require much more than warning users about risks and telling them the importance of adopting good behaviour. According to Bada and Sasse (2014), first of all people must be able to understand and apply the advice, and then they must be willing to do, and the latter requires changes to attitudes and intentions. Several psychological behaviour change theories such as theory of planned behaviour and protection motivation theory which are presented in the previous chapter are used to change employees' insecure password related behaviours in organisations. In addition to these methods, in recent years, persuasion approaches have been commonly used to motivate employees to behave in a secure manner.

To manage changing user behaviours which undermine password security in organisations, the current sources of persuasion along with organisational, personal, environmental and social factors need to be identified. There are more determinants such as cultural differences which can also influence the users' behaviour in organisations. However, within this chapter we primarily focus on organisational factors affecting users' password habits and practices thus the information security level of the organisations. Since the vast majority of behaviours are habitual, IT departments have a key role to support users to change from existing habits to better information security habits.

IT departments must influence and motivate employees to adopt secure behaviours. This requires more than simply telling people what they should do and should not do. In this chapter, first the factors affecting employees' password habits and practices will be identified. Then an empirical study will be presented to explore which factors most affect password security level in different organisations and how the related behaviour change theories and persuasion strategies can be utilised to improve the adoption of good password behaviour.

4.2 FACTORS INFLUENCING USERS' PASSWORD-RELATED BEHAVIOURS

Many organisations apply advanced information security technologies against the external threats. However, the main concern is related to internal threats caused by poor user behaviours (Leach, 2003). That 80% of security incidents in organisations are caused by internal threats is reported in a study (Boujettif and Wang, 2010). This proves that employees either intentionally or unintentionally cause many security breaches in organisations (Kreicberge, 2010; Siponen et al.,2010).

In this chapter, the factors affecting users' password-behaviour in organisations are categorized in three groups: organisational factors, motivational factors and education and awareness factors similar to the proposed information security framework by Soltanmohammadi, Asadi and Ithnin (2013). The following sections details these factors.

4.2.1 Organisational Factors

There are many organisational factors including policies, workload, environmental issues and organisational culture influencing information security in organisations. Many researchers investigated the significance of policy management, impact of effectual security applications and polices on information security and response of employees to the requirements of these policies (Fulford and Doherty, 2003; Karyda, 2005; Pahnila, 2007). Although these policies aim at forcing employees to act properly to increase system security (Sarriegi et al., 2006), they mostly have a reverse effect on security (e.g strict password policies to cause users to adopt coping strategies). One of the reason is that they cause more workload which is considered as an organisational factor affecting employees' behaviour (Kraemer et al., 2006; Kraemer and Carayon, 2007) Although, culture and social factors can impact the employees' behaviour and information security systems of organisations significantly, they are not our main focus in this study.

4.2.2 Motivational Factors

If users do not believe the information that is protected by the password mechanism accessed by themselves is at risk of being targeted, they will not be motivated to behave in a secure manner (Weirich, 2005). If users are educated about password security and aware of potential threats, they will behave in a proper manner. However, not only education and awareness but also usability issues of authentication mechanisms cause employees' lack of motivation. In most cases, authentication process creates an overhead for users. Users tend to cut corners to reduce extra load given a chance if they are not motivated to adopt secure password-related behaviours in organisations (Whitten and Tygar, 1999). For these reason, designing usable authentication schemes which will reduce the overhead is important.

On the other hand, employees show a better performance regarding security when they are controlled or monitored by leaders (Aarons, 2006). Leadership is a process to affect and motivate employees to follow rules. Many studies about leadership in organisations have revealed that it notably affects the employees' work performance (Kaushal, 2011 and Lo et al., 2010). Therefore, leadership plays an important role to direct

users and help them to fulfil with information security policies. IT specialists act as leaders regarding information and password security in organisations.

Personal factors also impact the employees' security-related behaviours. Their knowledge and understanding of security issues as well as their experiences, perceptions, attitudes and beliefs are the main influencers on behaviour (Coventry, et al., 2014). Personal motivation and personal ability, are the most powerful sources of influence (Patterson et al., 2011).

Rewards and punishment is another influencing method which can be used to increase employees' motivation to follow password policies. Rewarding people to do the right things makes them more security conscious. It should be used in conjunction with motivational strategies that encourage intrinsic satisfaction and social support (Kohn, 1994). However, rewards and punishment can have unintended consequences. Rewards for some employees who follow the standards may backfire, causing others to feel resentful (Patterson et al., 2008).

4.2.3 Education and Awareness Factors

Beyond monitoring and controlling employees, information security training has an important role on providing information security skills to employees. Users' knowledge and skills can affect their motivation to behave in a security-conscious fashion (Adams and Sasse, 1999). Information security training programs provide information about the importance of information system security to increase users' skill and understanding towards information security (Koskosas et al., 2011; Martin and Rice, 2011).

Information Security Awareness Campaigns:

Organisations need to secure their information assets and systems, and develop policies that specify the expected behaviours for their employees. They encourage employees by dispensing advice but major security failures continue to occur (Kirlappos and Sasse, 2012; Kirlappos, Parkin and Sasse, 2014).

Influence strategists need to identify behaviours which they wish to change before

they start trying to change them. Equally important is identifying the crucial moments when they are most likely to fail in meeting these goals (Patterson et al., 2011).

Awareness should not be perceived as training only. The purpose of awareness campaigns is simply to focus attention on security issues. They are intended to allow individuals to recognize IT security concerns and respond accordingly (Bada and Sasse, 2014).

4.3 THE EMPIRICAL STUDY: IMPROVING PASSWORD SECURITY BEHAVIOURS IN ORGANISATIONS

4.3.1 Introduction

A questionnaire and interview-based study has been conducted to investigate the impact of several factors on users' password behaviour. To evaluate the efficiency of several persuasion strategies on motivating employees to adopt good password behaviour and abandon coping strategies which puts organisations' information security into risks, a case study has also been performed.

To conduct the questionnaires and interviews an ethical approval was sought and obtained from the University of Sussex Sciences and Technology Cross Schools Research Ethics Committee (C-REC). The certificate of the ethical approval can be viewed in Appendix A.

The following sections presents the details of the empirical study.

4.3.2 Motivation of the Empirical Study

The purpose of this empirical study is investigating the reasons for employees' lack of motivation about protecting their passwords against potential security failures in organisations. There is a wealth of research demonstrating that, despite technical precautions taken by people within the organisations, undesired password-related behaviours cause organisations to lose confidential information.

In recent years, researchers started to use persuasion strategies, methods and

approaches to change those behaviours to improve information and computer security. This study utilised several persuasion strategies to eliminate employees' insecure password practices and persuade and motive them to behave in a more secure manner. To do this, firstly, underlying reasons to cause users' insecure password practices should be investigated and suitable methods should be applied to prevent possible security failures. For this purpose, in-depth interviews and surveys have been conducted with employees and IT specialists in different positions who use passwords to access important information in several organisations in Turkey.

In the previous chapter, several related behaviour change theories and persuasion strategies have been reviewed. Based on the review, several persuasion strategies which suit with the aim of the study have been chosen, and the efficiency of these strategies on users' password behaviour have been evaluated in this empirical study.

To use appropriate persuasion strategies to increase users' adoption of good password-related behaviour, thus increase the information security level of organisations is the main purpose of this study. Therefore, this study has utilised the authority and social proof principles of Cialdini's weapons of influence (Cialdini, 1988), in addition to rewards-punishment and fear appeal strategies. In order to determine whether these strategies have any effect on employees' password-behaviours in the organisations they have been asked related questions in a questionnaire. For example, to find out the impact of social factor principle on employees' password practices, participants of the study have been asked if their colleagues rewarded or punished for their password practices, how this situation would motivate them to behave. The questionnaire and interview questions can be viewed in Appendix A.

Considering the results of the questionnaire, a case study has been conducted to test the efficiency and practicality of these principles in real practices.

4.3.3 Methodology of the Empirical Study

4.3.3.1 The Design and Apparatus

The researcher has conducted questionnaires with the non-IT employees and interviews with the IT employees in several companies from different sectors. The

questionnaire and interview questions are different as the computer and information security background of the IT and non-IT employees are different. The study aims to reveal the differences of perceptions of the IT and non-IT employees about the importance of information security.

The participants were contacted via email or phone call to make an appointment to participate the study. The questionnaires and interviews have been conducted by the researcher mostly in the employees' workplaces.

The apparatus used in this study are as below:

- A questionnaire for the non-IT employees
- Interview questions for the IT employees
- Consent forms to read and accept for all participants

All the apparatus is included in the section Appendix A.

While the questionnaire given to the non-IT employees included 16 questions, the IT employees' interview included 10 questions. The questions were set to cover all important issues related to users' security behaviours from coping strategies to organizations' security mechanisms. The questions were clear to avoid the misunderstanding of the users. There are many studies on employees' security behaviour which used the similar approach, materials and questions in the literature (Beautement et al., 2016; Herath and Rao, 2009 and Weirich, 2005).

While the average time to complete the questionnaire was approximately 15 minutes, time to complete the interview was about 20 minutes.

4.3.3.2 The Procedure

At the beginning of the empirical study, all participants were given a brief information about the study and asked to read and accept the consent forms. For those participants who were interested in getting more information about the study researcher's contact information were provided in the consent form. Once the participants had accepted and signed the consent forms, they answered the questionnaire or interview

questions.

There was not any reward / incentive for participating this study.

The empirical study was finished by thanking to the participants for their participation.

4.3.3.3 Demographics

In this study, employees from different business areas have been asked a number of questions to find out the reasons for their insecure behaviours and how they would be motivated to behave in a secure manner. 121 participants from six sectors were recruited for this empirical study. 25 IT specialists have been interviewed and 96 non – IT employees have been given a questionnaire to fill out. In Table 4.1, number of the participants from each sector can be seen. Public sector refers to some government-affiliated institutions such as General Directorate of Highways in the experiment. Although the hospital is an organisation from public sector, it is classified as health sector in this study. All other organisations are private companies.

All the employees who participated in the study use passwords to access critical information in the organisations they work at. IT specialists who are interviewed have also been recruited from these organisations to see if there is a match between their perceptions of password security and other employees'.

The numbers of the employees from six sectors including banking, construction companies, health, insurance companies, public sector and software companies indicates the numbers of non-IT employees from each sector. However, the number of IT employees (N=25) indicates the total number of IT employees from all sectors (see Table 4.1). The data collected from the IT employees is analysed separately (see Figure 4.8). This data is not included in the data analysis of the non-IT employees (N=96) since the interview questions of the IT employees and the questionnaire questions of the non-IT employees were different. The questionnaire and interview questions can be viewed in Appendix A.

The data collected from the interviews of the IT employees were also used to

conduct the case study (see section 4.3.5). 7 non-IT employees from software companies should not be confused with the IT employees. Non-IT employees from software companies work in research and development departments and they are not responsible for the duties of IT employees.

Table 4.1 Number of the participants from all sectors

Banking	*Construction Companies*	*Health*	*Insurance Companies*	*Public Sector*	*Software Companies*	*IT*
14	11	41	7	16	7	25

Most of the participants were male. The demographic details of the participants can be seen in Figure 4.1 and Figure 4.2.

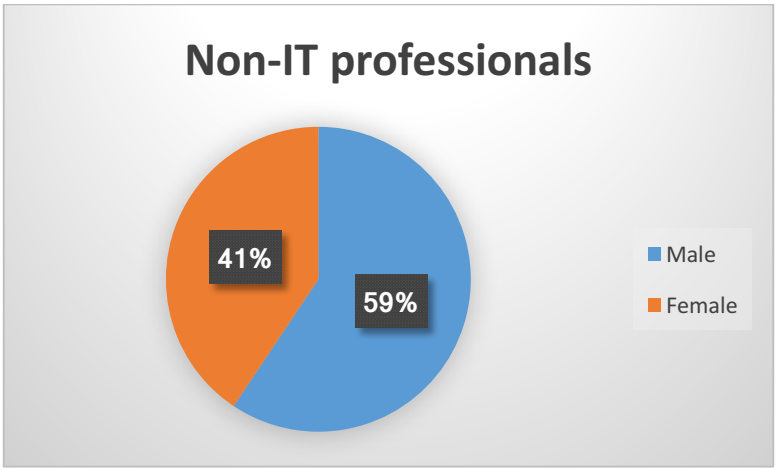


Figure 4.1 Gender percentages of the non-IT employees

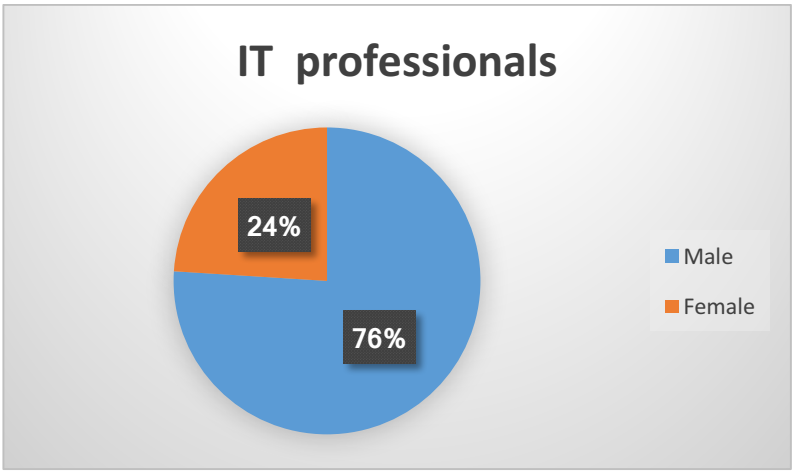


Figure 4.2 Gender percentages of the IT employees

4.3.4 The Results and Analysis of the Empirical Study

This section presents the results of the empirical study based on the employees' and IT specialists' responses to questions.

***Frequency of Password Change**:*

In all organisations involved in this study, information security and privacy issues were quite important and additionally, any hacking or leak would be consequential. For instance, while all participants from the hospital can access the private health information of patients, participants from banks can view the bank account details of their customer. All this information is protected with a password. Changing the passwords used for access to organisational information frequently is a requirement for employees. However, password change requirements implemented by the systems were different in each organisation. For banking employees, password change policies were most strict, they were required to change their passwords on a monthly basis. On the other hand, for construction companies and health professionals, there were no regular password change requirements. Insurance Company and Public Sector employees were changing their passwords every six months. And the software company employees were asked to change their passwords once per year (see Table 4.2).

Table 4.2 Frequencies of Password Change Requirements in Each Sector

Banking	*Construction Companies*	*Health*	*Insurance Companies*	*Public Sector*	*Software Companies*
Every month	No password change requirement	No password change requirement	Every six months	Every six months	Every year

Use of Coping Strategies:

Employees from six sectors were asked whether they use the following three coping strategies; sharing passwords, using similar passwords or reusing the same passwords, and writing down their passwords (see Figure 4.3).

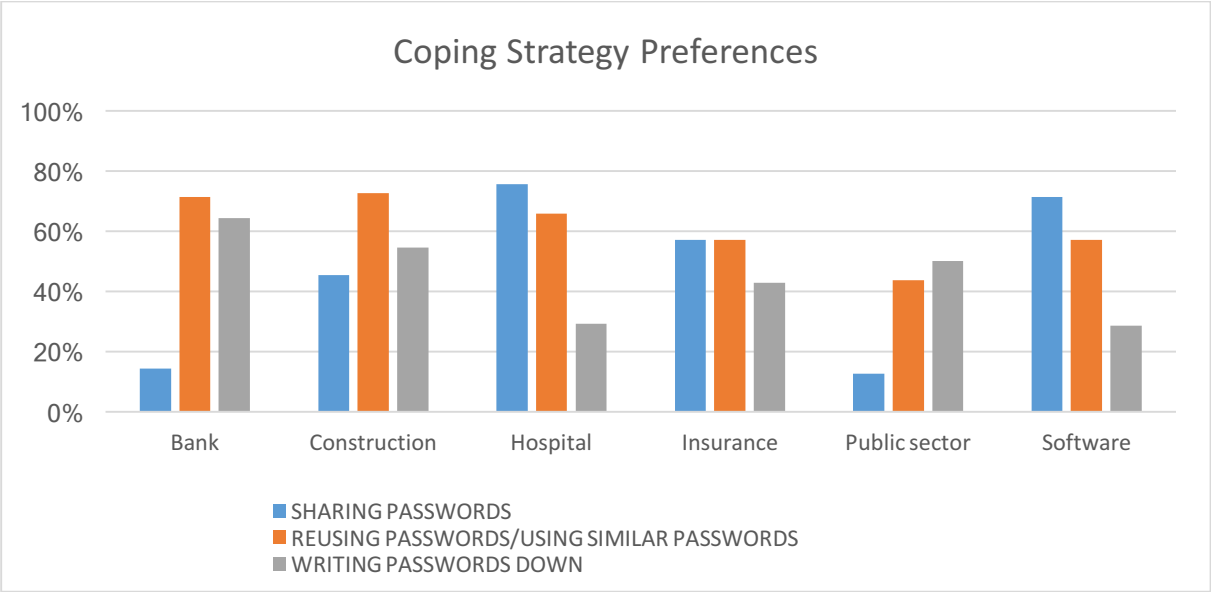


Figure 4. 3 Preferences of coping strategies with the passwords in each organisation

Chi-square analyses yielded significant results only for sharing passwords, Likelihood Ratio $\chi^2(2, N = 96) = 30.854$, $p < .001$. This difference mostly comes from the hospital and software company employees. 31 out of 41 hospital employees and 5 out of 7 software company employees reported that they shared their passwords with others, while in other groups, half of the participants or less were in favour of sharing passwords.

There were no significant differences between sectors in terms of password reuse behaviour (Likelihood Ratio $\chi^2(2, N = 96) = 3.682$, $p = .596$) or in terms of writing passwords down (Likelihood Ratio $\chi^2(2, N = 96) = 7.309$, $p = .199$).

Apart from the specific coping strategies preferred, the number of the strategies used is also important. Only 11 % of the participants who attended this study reported no use of any coping strategies. Most of the participants use one or two coping strategies (72 %, see Figure 4.4).

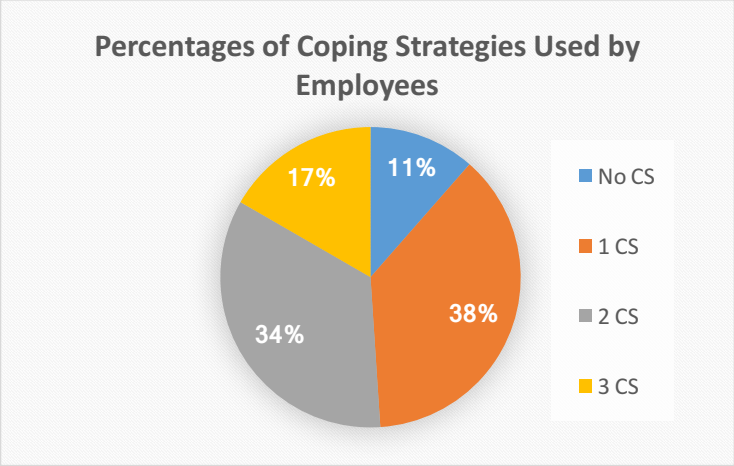


Figure 4. 4 Distribution of employees according to their use of coping strategies

Additionally, the number of coping strategies used by employees of different sectors can be seen in Figure 4.5. Most of the construction company employees seemed to use two or three strategies (see Table 4.3). Similarly, all health industry employees preferred using coping strategies.

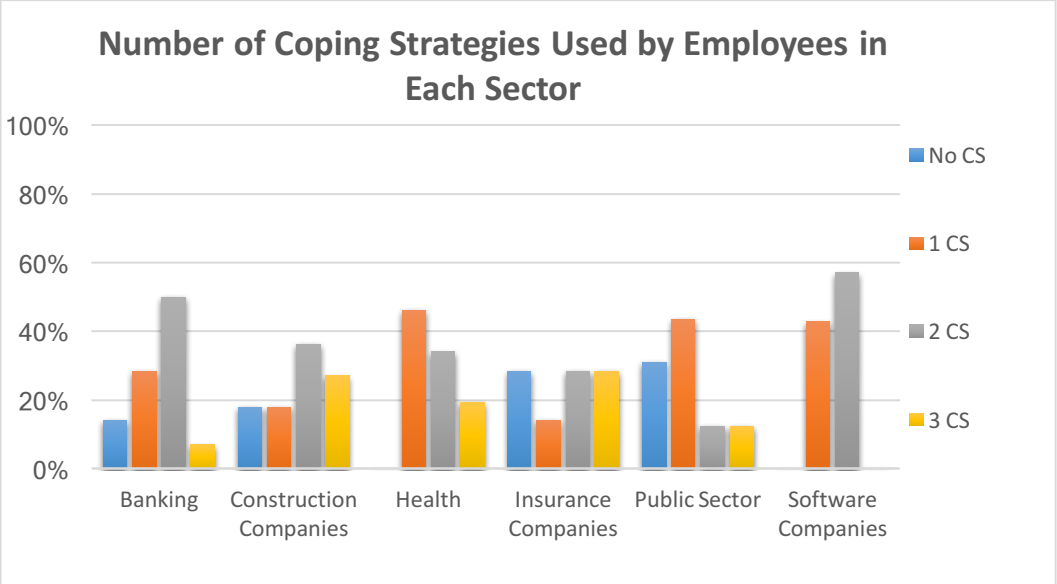


Figure 4. 5 Numbers of coping strategies used by employees in each sector

Training:

Some people in the sample were trained on the importance of information security. Table 3.3 shows the percentages of people who had training about password security.

Table 4.3 Number of Employees with Information Security Training in Each Sector

Banking	*Construction Companies*	*Health*	*Insurance Companies*	*Public Sector*	*Software Companies*
71%	0%	7%	0%	44%	71%

Moreover, training impacted people's insecure password behaviour as Figure 4.6 illustrates.

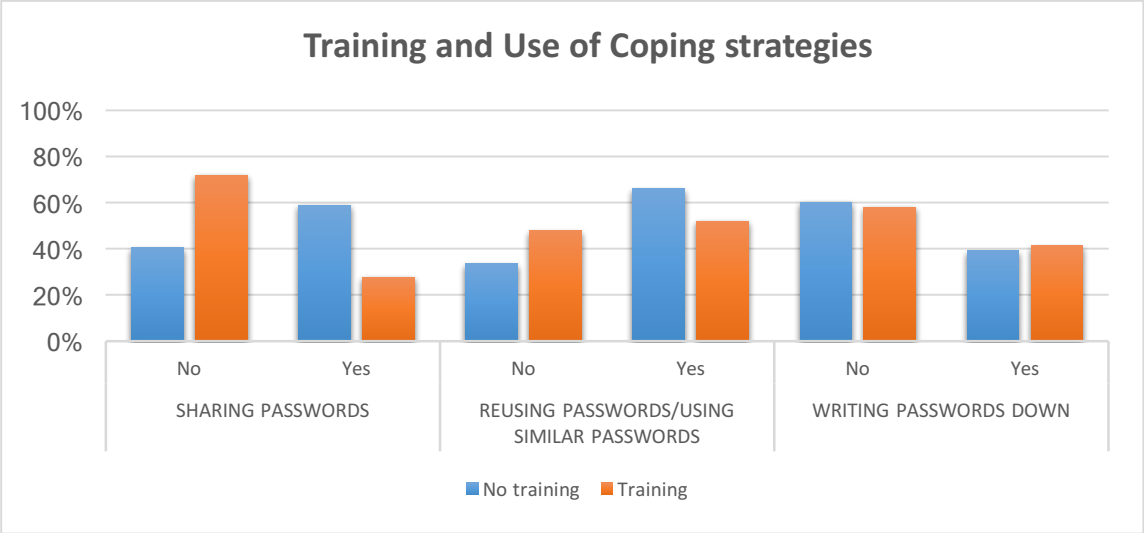


Figure 4. 6 Impact of password security training on adoption of coping strategies

Chi-square analyses showed that those who had a training on information security are less likely to share their passwords such that 72% of those who had training did not share their passwords and 59 % of those without a training share their passwords (χ^2 (1, N = 96) = 7.182, p = .007). Training factor did not yield a significant result in terms of reuse of passwords or using similar passwords (χ^2 (1, N = 96) = 1.590, p = .207). Similarly, training did not make any difference in terms of writing down the passwords either (χ^2 (1, N = 96) = .558, p = .455). Additionally, most of those who had a training (84%) did not consider lack of training as a potential cause of insecure password behaviour whereas 65 % of those without training mentioned lack of training as a potential cause, and the difference was statistically significant (χ^2 (1, N = 96) = 17.635, p < .001).

Reasons for Insecure Password Practices:

Five potential reasons were investigated in terms of their impacts on adopting poor security behaviours. In this empirical study, the usability issues of security mechanisms refer to password creation policies of the organisations and user interface of used authentication schemes. Although, they can be categorized as organisational factors they are evaluated separately in this study. Workload is evaluated as the organisational factor.

When participants reported whether they agreed or not with mainly five reasons for insecure password behaviour (See Figure 4.7), personal factors were the least attributed cause among others.

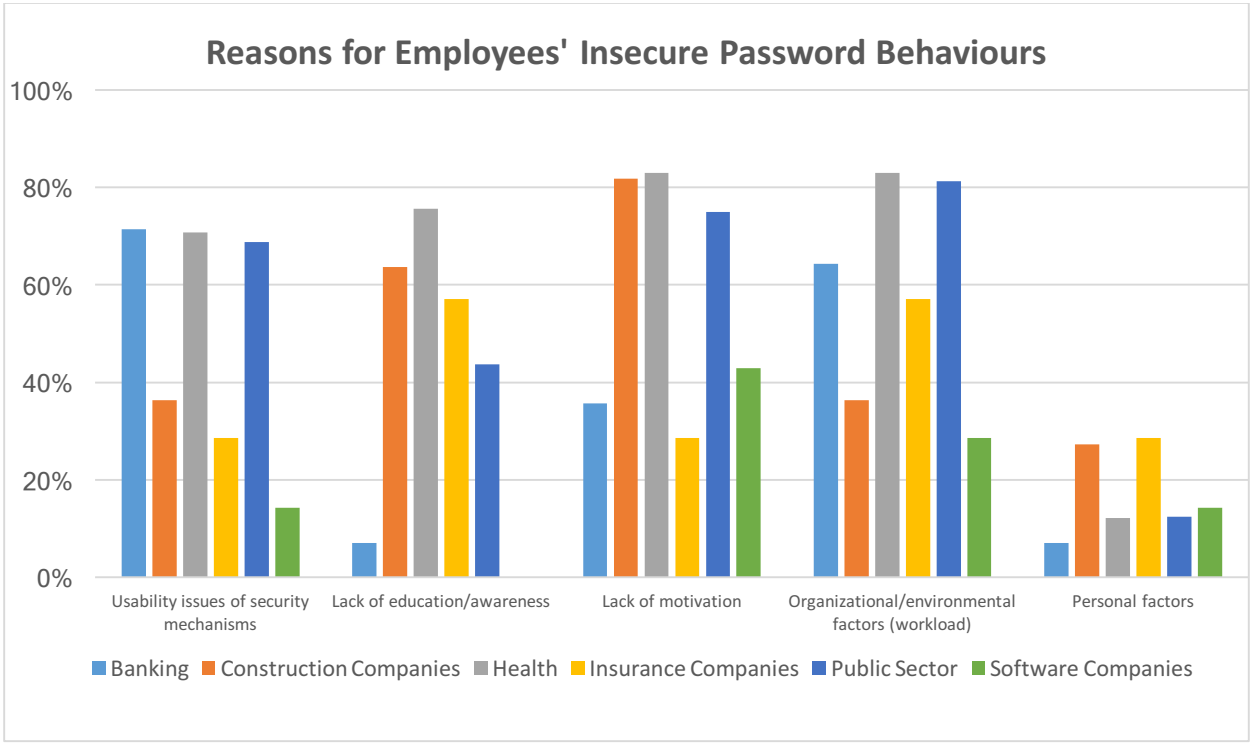


Figure 4. 7 The reasons for employees' insecure password behaviours

Those working in the software industry attributed insecure behaviour least to the usability of mechanisms. This trend was quite similar for the IT professional (See Figure 4.8). Only 16 % of all IT professionals agreed that usability issues were also a cause for the insecure password behaviour. Most of the IT Personnel considered lack of education (72%) and lack of motivation (56%) as the potential reasons for it. Construction companies also followed this trend (64% and 82% respectively). In the banking sector, the main reasons were usability issues (71%) and workload (64%). Health professionals rated all factors except personal factor with highest agreement. Across all factors, more than 70 % of the health professionals identified the given concerns as potential causes of insecure password behaviour.

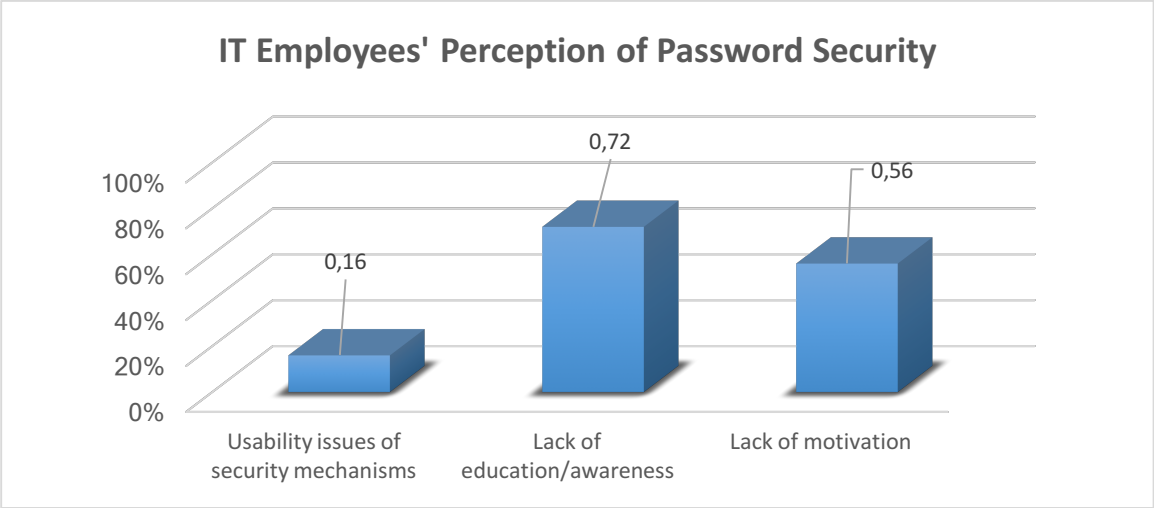


Figure 4. 8 Reasons for employees' insecure password behaviours according to IT specialists' perception

Improving secure password behaviour:

Training on password security, usable password mechanisms, personal beliefs on ethics to maintain privacy of information as well as several persuasion strategies such as social proof, fear appeal and rewards and punishment have been evaluated to find out whether they have any effect on motivating employees to adopt good password behaviours.

The question asked to participants in the questionnaire in relation to each strategy/method were as follows:

Which one of the followings would motivate you to abandon insecure behaviours (sharing passwords etc.) and adopt the good ones?

User Education: If you were trained about the password security in organisation.

Usable Password Mechanisms: If you were using usable password mechanisms (e.g. password policies or guidelines which allow you to create memorable and strong passwords)

Reward and Punishment: If you were punished for your insecure behaviours or rewarded for the good behaviours.

Ethical Issues: If you personally believe that to care protecting privacy of information you access via password is an ethical behaviour.

Fear Appeals: If you received a message from IT department informing you about the potential threats to passwords, and consequences of your careless behaviour.

Social Proof: If you witnessed that your colleagues care to protect their passwords.

According to responses, all industries considered training as a potential solution more or less (all above 29%). The first three industries in Figure 4.9 believed more in training, and the difference were approaching statistical significance, Likelihood Ratio χ^2 (5, N = 96) = 9.437, p = .093.

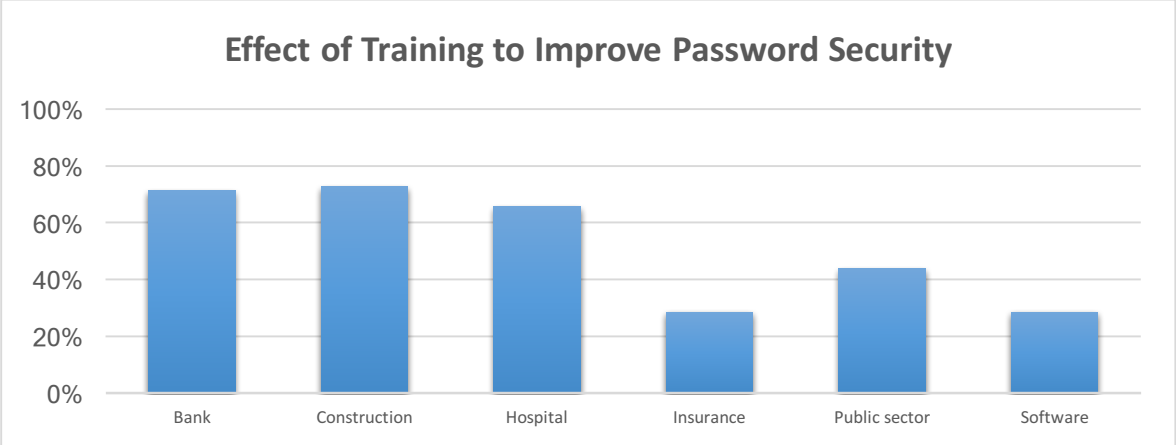


Figure 4. 9 Effect of training on motivating employees from different organisations to adopt secure password behaviours

For the usability of the mechanisms, sectors significantly differed (Likelihood Ratio χ^2 (5, N = 96) = 27.440, p < .001. Banking, Health and Public Sector employees reported that usability of security mechanisms would impact secure password behaviour (all above 75%) whereas those who worked in more tech related jobs disagreed on this solution (all up to 29 % agreement). Figure 4.10 shows the effect of usable password mechanisms on employees' motivation adopting secure password behaviours in each organisation.

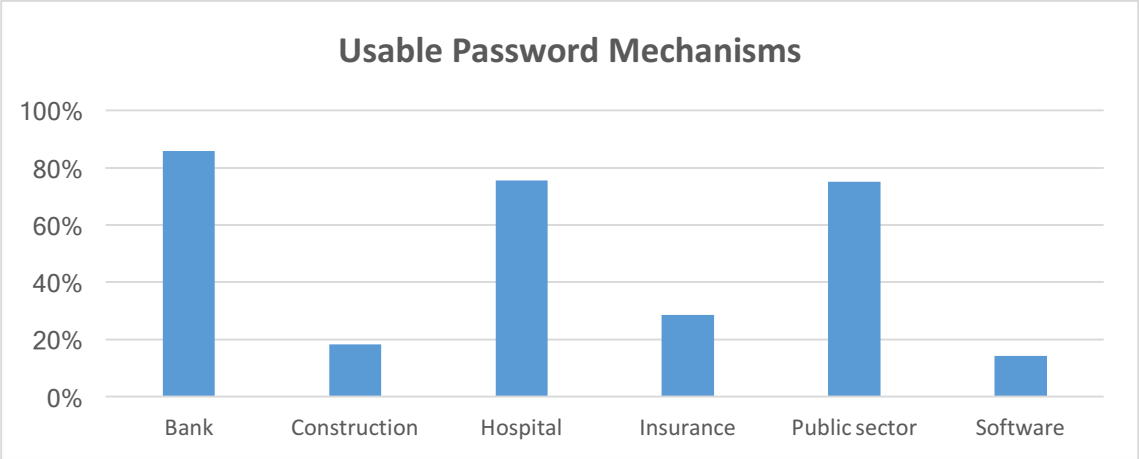


Figure 4. 10 Effect of usable password mechanisms on motivating employees from different organisations to adopt secure password behaviours

Other social and personal factors were also evaluated based on participants' responses on the related questions. Results show that, reward and punishment methods would be a solution for insecure password behaviour according to employees from all sectors except hospital employees (>70% vs. 12%; Likelihood Ratio χ^2 (5, N = 96) = 50.429, p < .001). Participants' personal beliefs regarding the importance of information privacy was a potential motivation for bank employees (71%) and similarly for insurance company employees (57%), Likelihood Ratio χ^2 (5, N = 96) = 15.353, p = .009. Although health information should be kept private, unfortunately less than half of the participants from the hospital gave importance to this.

People from all industries agreed that fear appeals would improve secure behaviour (all above 71% and not significantly different from each other, Likelihood Ratio χ^2 (5, N = 96) =1.581, p = .904). Similarly, most of the participants agreed that social proof would improve secure behaviour (all above 57 % and not significantly different from each other, Likelihood Ratio χ^2 (5, N = 96) =1.582, p = .903). Figure 4.11 illustrates the effect of the aforementioned strategies on employees' password-related behaviours in each organisation.

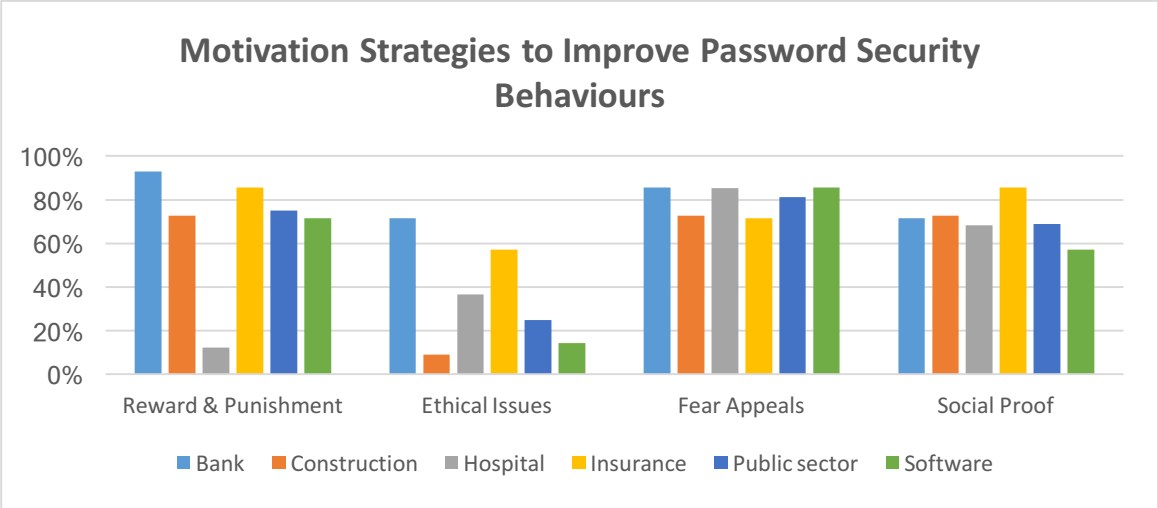


Figure 4. 11 Effect of other motivation strategies on employees' password-related behaviours in organisations

4.3.5 Case Study: Password Security in the Hospital

According to questionnaire results and IT experts' statements, the hospital employees are the less motivated participants about protecting their passwords in this experiment. Therefore, the researcher and the IT crew of the hospital worked together to utilise some persuasion approaches to increase the employees' motivation. During two months, their password practices were observed to understand whether the applied strategies made a positive change on their behaviours.

Most of the employees of hospital and software company reported that they shared their passwords with others, while in other groups, half of the participants or less were in favour of sharing passwords. The reason of this situation is that the participants from the software company mostly work on the same projects so they share their passwords to contribute to the project. As they share the responsibility for their work, this might be acceptable. However, the situation is quite different in the hospital. The most common scenario is that the attending physicians share their passwords with their assistants, junior doctors or interns, and ask them to enter the patients' medical information including prescribed medicines to the computer. However, only the attending physicians is authorized the prescribe medicines. This sometimes caused the wrong prescriptions which put the patients' health into a serious risk. The IT department alleged that password sharing habits did not seem to be decreased although some patients sued the doctors in

the past. Probably most of the employees do not think that it happens to them until they face the same situation. The IT crew also stated that most employees do not lock the computer screen and even unauthorised people can see the patients' medical information. To raise awareness of the consequences of such behaviours, employees have been first sent an email informing them about the past password failure events by the IT department. The email included advises for employees to choose stronger passwords, and not to share their passwords with colleagues. The employees were also informed that in similar cases, the employees will be accused of neglecting the privacy of patients' health information and will be reported to the manager from now on. In the following two weeks 28% of the employees in the organisation changed their passwords including the ones who used the same password since they started the work.

The next approach was punishing the employees who did not lock the computer screens, sharing their passwords with the colleagues while they are away from hospital. However, it was difficult to control these behaviours so no positive change in behaviours was observed.

During the process of motivating employees, the other approach was organizing a password security seminar to raise awareness of the password security issues. According to IT department, attendance at information security themed seminars was very low in the hospital. However, this time the employees were sent an invitation e-mail informing that an information security expert will attend the seminar and give critical information about the importance of password security to protect patients' medical records. The attendance was at least 20% more than ever.

These exercises showed that fear appeals and authority principles are effective to motivate hospital employees to change their poor password behaviours with the good ones.

4.4 DISCUSSION

The aim of the empirical study is to investigate whether persuasion strategies can be applied to promote secure password-related behaviour among employees in organisations. Several appropriate strategies are selected in order to suit the aim of the

study. The questionnaire and interview results and outcomes of the case study shows that two principles of Cialdini's weapons of influence (Cialdini, 1988), social proof and authority, is effective on motivating employees to adopt better password behaviours. Apparently, most of the participants are influenced by their colleagues' secure password behaviour and they are encouraged to improve their own behaviours.

The results of the case study showed that when participants were sent messages informing them about the possible threats and mentioning the consequences of their insecure password practices, they are more likely to be motivated on choosing secure password behaviours. This proves that fear appeal is also a significant motivation for most employees almost from all sectors.

According to results related to training, most of the employees who did not have any training about the information / password security before seemed to use two or three coping strategies such as sharing passwords or writing them down. For this reason, password and information security training must be compulsory for all employees from each sector, especially for those who access to the critical information like participants in this study. This training might be the part of orientation programs of the organisation given to the potential employees before they start to work.

On the other hand, the motivation strategies should be chosen and applied considering the organisation culture and the nature of the jobs. Password policies should be specialized for each organisation since requirements of the job and environmental factors differ in each organisation.

The results of the empirical study show that persuasion is a powerful tool for attitude or behaviour change, and can be applied in real life practices to promote secure password-related behaviour.

This study contributes to password policy compliance research, so it might be influential for IT specialists, experts on awareness campaigns, influence strategists as well as policy writers.

There are, however, some limitations of this study. There is a possibility that a proportion of participants might have underreported their bad password behaviours undermining information security in the organizations. The presence of the researcher

while collecting the data may have affected the participants' answers. This means that taking self-reports on past and future behaviour of the participants at face value might have reduced the accuracy of the results. Also, it would be better to conduct this study in some organisations in another country to be able to make a comparison with Turkey. In the most organisations involved in this study, there was not adequate training on security awareness so most of the employees were either untrained or poorly trained about the information security. An empirical study conducted with employees with a solid background in security awareness might yield different results.

4.5 SUMMARY

This chapter primarily identified the factors influencing password security-related behaviours of employees in different organisations where their password practices are under control of the IT departments. Then it focused on the motivation methods to persuade employees to abandon several coping strategies with the passwords, and improve password security behaviour in organisations. Writing down passwords or keep them somewhere accessible, sharing them with colleagues and reusing same passwords across different accounts were some of these strategies which potentially cause security failures by increasing the chance of obtaining passwords by third parties.

Weak password selection is also a significant reason of password security failure. This study revealed that the password policies and guidelines used by the organisations are not adequate to guide users to select strong passwords and adopt good password behaviour. On the contrary, using unnecessarily restrictive password rules tend to make it much easier for an attacker to compromise user credentials. Therefore, the next chapter investigates the problems with the existing password guidelines and propose usable solutions to these problems.

CHAPTER 5

CREATING SECURE AND MEMORABLE PASSWORDS

5.1 INTRODUCTION

As described in the previous chapter, human factor has a key role in password security. However, security problems caused by user behaviour has not been totally solved. This chapter investigates the effect of password policy rules on users' password-related behaviours and password preferences. As previous studies proved that existing password policy rules are not adequate to motivate users to choose strong passwords, this chapter presents the idea of including several password creation methods in password guidelines and also adding motivating elements to the password creation process without enforcing any restriction rules.

Initially, this chapter presents the previous studies on password guideline domains. An empirical study has been carried out to evaluate the efficiency of the proposed password guideline. In the study, security and usability of the proposed password guideline including a persuasive text message and several password creation methods were compared with the usual password policy rules.

Details of the empirical study including the design, measurements, apparatus and procedure will be presented in the following sections. Then the findings will be discussed, focusing on the efficiency of proposed password guideline on improving the strength of the users' passwords as well as the compliance behaviour.

5.2 BACKGROUND

Despite the development of various alternative authentication mechanisms such as smart cards, tokens, graphical passwords and biometrics, textual password based authentication remains prevalent (Campbell, Ma and Kleeman, 2006). Rather than technical problems in the password system itself, human behaviours and users' password practices cause more vulnerabilities.

To increase the strength of user chosen passwords, users typically require to adhere to a set of rules known as password guideline when creating passwords (see section 2.5.2) Users compose their passwords following the specific requirements in password guidelines. For example, the password must contain at least eight characters including at least one number or one upper case letter, and it should not contain the username. There are various password guidelines that are used by organisations. They should be written efficiently to provide adequate security levels in the organisations (Summers and Bosworth, 2004; Campbell, Ma and Kleeman, 2006).

Since only a few studies have been conducted about the construction of password guidelines so far, there is lack of empirical data on the guidelines and passwords which were created complying with them (Komanduri et al., 2011). For example, there is not sufficient numbers of experimental studies conducted to evaluate the NIST guidelines (Burr, Dodson and Polk, 2006) which are used to produce password composition policies. They are still mostly based on theoretical estimates. Zakaria (2013) conducted a laboratory-controlled experiment to test the compliance to NIST guidelines by different experimental groups which were given different persuasive rationales based on their personality differences. Although investigating the effect of personality variables on susceptibility of users to persuasion, it is difficult to draw a firm conclusion. Evaluation of efficiency and security of some other guidelines are also based on very small-scale laboratory studies (Proctor et al., 2002; Vu et al., 2007).

The content of password guidelines should be created carefully as it is important in providing suggestions and instructions to users on how to create good passwords. Grawmeyer and Johnson (2011) conducted a study to investigate users' password generation behaviour. All the passwords estimated as highly secure and secure in the study were in fact insecure passwords containing a single word. Therefore, the authors suggested that password guidelines contained in security policies should be devised and founded on a sufficient theoretical understanding of the users' task.

Previous research showed that strict password policy rules do not increase the password security as what is believed (Inglesant and Sasse, 2010; Komanduri et al., 2011; Summers and Bosworth, 2004). Users adopt coping strategies such as writing passwords down or sharing them when they are imposed to use those rules to compose their passwords. Even if they do not, most of the passwords created by complying with

password policy rules are still not strong enough. However, it might be possible to create strong and memorable passwords by changing the content of password guidelines.

Therefore, the purpose of this study is to guide users to create stronger passwords to improve password security providing several password creation methods in password guidelines instead of usual password policy rules. People who are particularly interested in doing research to increase the strength of their passwords and create complex passwords can find many password creation methods and tips on the web to help themselves. However, since most of the users tend to ignore security precautions and they are not interested in doing research about the security, including these methods in password creation process, should be more influential and efficient. Thus, they would see how to create strong and memorable passwords correctly before they create their own. The methods provided to users in the study inspire users to create their own formula which they can use to turn any simple word to a complex password.

This study also investigates the effect of a persuasive text provided to users on the password creation process to encourage them to create their unique password creation formula on password strength. The existing password guidelines only focus on providing information on how to compose a good password. According to Cialdini (2001), people will more likely comply with a request when they are provided a rationale. Accordingly, a study revealed that a password guideline including a rationale as to why choosing strong password is important indeed improved the password compliance (Zakaria, 2013). However, this study aims at not only telling people what is important and what should be done to increase password security but also show them how to do it. Therefore, users are provided a persuasive message along with the example methods. In fact, one of the most important component of persuasion is free choice (Perloff, 2003). Accordingly, the proposed password guideline allows users to be free to create their own strategy on composing passwords. It means that the example methods aim to inspire users to create their unique encryption formula.

Briefly, this study seeks to discover if users will create strong and memorable passwords when they are provided several password creation methods along with a persuasive message, without imposing them any password policy rules.

The next section describes the empirical study which was conducted to evaluate

the proposed idea.

5.3 THE EMPIRICAL STUDY: PERSUADING USERS TO CREATE STRONG AND MEMORABLE PASSWORDS

5.3.1 Introduction

A web-based empirical study was carried out to investigate the assumption that users can create stronger and more memorable passwords if they are not enforced to comply with strict password policy rules. The study evaluates the effect of several password creation methods on the strength and memorability of users' passwords. It also explores the users' password behaviour and practices in either cases: with and without following strict password policy rules.

To perform this study an ethical approval was sought and obtained from the University of Sussex Sciences and Technology Cross Schools Research Ethics Committee (C-REC). The certificate of the ethical approval can be viewed in Appendix B. The following sections presents the details of the empirical study.

5.3.2 Methodology of the Empirical Study

5.3.2.1 The Design and Apparatus

The empirical study used the between-subject design where participants can be part of the experimental group or the control group, but cannot be part of both. There is one control group and one experimental group in the study. The strength and memorability of the passwords created by participants in each group were measured and compared to each other. While the participants in the control group were given some password policy rules to be followed when creating their passwords, the participants in the experimental group were given several password creation methods as examples to create their own encryption formula to compose their passwords without being have to apply any rules.

Two websites were created to collect data for this empirical study: one for the experimental group and one for the control group. The apparatus used in this study are as below:

- A password guideline including five password composition rules for the control

group,

- A password guideline including three sample password creation methods and a persuasive message and important notes for the experimental group
- A password register/login page of a web site for the control group
- A password register/login page of a website for the experimental group
- Two sets of questionnaires: one for the control group and one for the experimental group
- Consent forms to read and accept for all participants

All the apparatus is included in the section Appendix B.

Once the participants in each group had signed up their websites, they were provided a message and a survey link directing them to another website to fill a questionnaire. While the questionnaire given to the control group included 19 questions, experimental group's questionnaire included 30 questions. The questions in the control group's questionnaire were common for both group. The average time to complete the questionnaire was approximately 15 minutes for the experimental group and 10 minutes for the control group.

As stated above, the password guidelines which were distributed to the participants are different according to the group to which they were assigned. The participants in the control group received a set of password composition rules are as below:

The password composition rules for the control group:

- Your password must be at least 8 characters long.

- Your password must contain at least one upper case, one lower case, one number and one special keyboard character.

- Your password should not contain your username.

- You should use different passwords across different accounts.

- Your password should not be easily guessable.

The participants in the experimental group were given a persuasive message telling them that it is possible to create strong and memorable passwords applying some methods. The message attempts to persuade participants to create a unique formula thus they could turn even a simple word to a complex password which is hard to crack. In addition to this message, participants in the experimental group were also given these methods with examples. The password guideline of the experimental group was framed using logical reasoning by providing explanations such as the fact that if users create weak passwords for ordinary websites, a crafty hacker can obtain that password easily. If using the same or similar password is the user's habit so it would not be difficult for the hacker to guess the other passwords created for important accounts such as bank account.

The password guideline including the persuasive message and password composition methods given to the experimental group are as follows:

YOU CAN CREATE VERY STRONG PASSWORDS WITH SIMPLE AND MEMORABLE METHODS TO PROTECT YOUR ACCOUNTS! PLEASE READ CAREFULLY AND UNDERSTAND THE LOGIC OR BASES OF THE METHODS.

Before signing in, please use the methods given below to create your password. These methods offer a high level of security by leading you to create your own encryption formula to produce strong passwords from memorable words. Once you have understood the encrypting logic behind the manipulation of memorable words with equally memorable strings of numbers to create your very own formula, you will be able to transform words and numbers that are memorable for you, into very strong passwords. Memorable words mixed appropriately with memorable strings of numbers leads to strong passwords.

Important Note: You should choose words and numbers unrelated to your personal details. For example, don't encrypt your name or surname. And don't use strings of numbers that indicate your date of birth. Even though others do not have a clue about your formula, it is risky.
Remember that password selection is very important to protect your confidential data. Without exception, you should care about your password selection for anything from ordinary websites to bank accounts. A crafty hacker can easily obtain your weak password within seconds. Also remember that if you use very similar passwords across different accounts, and, once the hackers have obtained one of your passwords, they can easily guess the others.
Below are examples of workable methods. You should not apply exactly any of the examples as your own password. The examples are given only to show the possibilities of good encryption formulation that consequently lead you to think of your own encryption formulation resulting in a memorable formula.

Method-1:
Step 1: Pick a word. Let's say, "education" as our plain password.
Step 2: Specify a number. Let's say, 347.
So we have the word "education" and the number "347". Let's encrypt them.
Step 3: Convert the 3rd, 4th and 7th letters of the word "education" to upper case. We now have "edUCatIon".
Step 4: Place the numbers 3, 4 and 7 after each of the upper case letters. This gives us "edU3C4atI7on".
Step 5: Change the value of each of the numbers in Step 4 by increasing or decreasing each. In this case, we will choose to increase each by 2. Therefore 3 + 2 becomes 5, 4 + 2 becomes 6 and, 7 + 2 becomes 9. So now we have the strong password **edU56atI9on**.
That's it! It is almost impossible to guess and very hard to crack. You can even write the plain password somewhere to help you remember it. As long as no one knows your formula that converts a plain password into a strong password, plain passwords are meaningless to them.
Here's another example. Let's pick a Turkish word and the number 148. Our plain password here is "bilgisayar". When we applied the same formula, this plain password converts into the strong password **B3ilG6isaY10ar**.

Method-2:
Step 1: Choose a string of plain numbers. Let's choose the numbers "12345".
Step 2: Specify a combination of letters and keyboard characters. Let's specify "m_y_". (Letters separated by underscores).
Step 3: Mix the string of plain numbers with the combination of letters and keyboard characters. In this case, we sequentially alternate the individual numbers of Step1 with the letters and keyboard characters of Step 2. Thus, we get the strong password **1m2_3y4_5**.

Method-3
If you want to use meaningful words and phrases you have to create a very long password combining letters, numbers and other keyboard characters. For example, **"myfavouritechicredshoes-size4"**. This phrase is meaningful to you, so you can remember it easily, but for other people it should be hard to guess. You can combine unrelated words which you can associate. An example of this is **"elephant.zoo.travel.Africa"**. An elephant might remind you of a zoo and a travel to Africa.

Important Notes:
- You can pick a related simple password or add some more characters to your encrypted password to remind you of the site for which you create the password.
- You should not use the same examples and/or formulas given in the above methods. You should create your own.
- You should use different passwords for different accounts.
- You should never share your passwords and/or your formula with anyone.
- You can apply your formula to different words and numbers to create different passwords.

The participants were shown a register/login page to enter their username and password. At the beginning of the empirical study, the participants were assigned a unique ID number. The interfaces of the register/login page are as illustrated in Appendix B.

The last apparatus involved in the study is the questionnaires of the control and experimental group. The control group's questionnaire contains several questions on demographic details of the participants and some questions related to password constructions and usage. In addition to these questions, experimental group's questionnaire contains some questions to find out the user satisfaction with the given methods and the effect of the methods on users' password choice. The questionnaires can be viewed in Appendix B.

The questions in the questionnaires were set to understand the reasons for the participants' password practices and determine the influence of proposed password guideline on password strength and memorability. A pilot survey was conducted before with fewer participants to test the quality of the questions. The content of several questions in the preliminary questionnaires were changed to better suit the aim of the study. Also, some previous studies were reviewed that used the several materials and questions (Shay et al., 2010 and Zakaria, 2013).

5.3.2.2 The Procedure

At the beginning of the empirical study, all participants were automatically assigned a unique id number. This id numbers were used to match the participants' credentials and questionnaire responses. The participants in the both group were given a brief information about the study and asked to read and accept the consent form to participate. Once they had accepted the consent form, they were able to sign up their website. For those participants who were interested in getting more information about the study researcher's contact information were provided in the consent form. As presented above, participants received different password guidelines while signing up. After the participants signed up the websites successfully, they were asked to click the provided link which would direct them to the survey website to fill the questionnaire. Before filling the questionnaire, a brief introduction was provided to participants informing them about the approximate time which the questionnaire would take. Finally, the empirical study

was finished with a message of thanks to participants for their participation.

The participants were asked to login the websites after a week and a month to find out whether they recall their passwords. At the end of the study, five randomly chosen participants were awarded £20 for the time and effort in participating.

The procedure of the study was exactly same for both groups except the password guidelines and additional questions in the experimental group's questionnaire.

5.3.2.3 The Measurements

There are several measurements involved in the empirical study: password strength, password length, memorability, password policy compliance, use of the given methods, user satisfaction and persuasiveness. The password strength was measured using tools known as the "*Password Meter*" (Password Meter, n.d.) and "*How Secure is my Password?*" (Collider, 2016).

Password Meter measures the password strength using a combination of several important attributes that constitute a particular password, such as length (i.e. number of the characters), the frequency of uppercase, lowercase, numerical characters and alphanumeric characters (i.e. punctuation and mathematical symbols). Password strength calculation is made by adding points if the password meets the requirements, and deducting points if not. The tool categorizes the passwords by giving scores where the maximum score is 100% according to complexity of the password. The passwords will be categorized as follows: very weak (0% < password score ≤ 20%), weak (20% ≤ password score ≤ 40%), good (40% ≤ password score ≤ 60%), strong (60% ≤ password score ≤ 80%) and very strong (80% ≤ password score ≤ 100). The measurement criteria and the categorization used to determine the password's strength can be referred to in Appendix B.

How Secure is my Password? measures the time in which the password entered could possibly be cracked by a computer. The tool takes into consideration the length, whether the password given looks like a dictionary word and the character variety while measuring the estimated cracking time.

The next element that was also measured in this study is the memorability. To evaluate the recall rate, the participants were asked to login to the websites after a week and after a month. To carry out the measurement of memorability, participants were given numbers where 0 indicates that user could not login successfully, 1 indicates that user logged in successfully in the first attempt and 2 indicates that user logged in successfully after a few attempts.

The other measurement in the study was password policy compliance. Since the participants in the control group must follow the given password policy rules, the measurement was conducted to find out whether the participants in the experimental group applied these rules to their passwords. Passwords were given scores for each requirement where 0 indicates that the related rules had not been applied, and 1 indicates that the related rules had been applied by the participant. Briefly, the measurement showed how close each participant in the experimental group followed the requirements given in the password guideline of the control group.

Use of given methods, user satisfaction and persuasiveness were measured based on questionnaire responses of the participants in the experimental group to evaluate the password guidelines given them.

Next section presents the demographics of the participants in the study.

5.3.2.4 Demographics

308 people participated in this study. 152 of them were in the experimental group and they created passwords after reading a persuasive text on how to create strong and memorable passwords. 156 people were in the control group where they had to follow five commonly used instructions to create a password. 142 people in the experimental group and 95 people in the control group filled out a follow up questionnaire including questions about their password creating habits and their thoughts of given methods. Therefore, demographics and survey analyses were run for 237 participants whereas password strength, compliance and memorability scores were analysed for all 308 participants.

The participants are recruited from college students studying in some universities in UK, USA and Turkey. Undergraduate students as well as the postgraduate students

participated in the study. Some of the participants have computer science related background.

There were 111 females and 126 male participants. 90.8 % of the experimental group and 86.3 % of the control group were aged between 18-35 years. Figure 5.1, 5.2 and 5.3 illustrate the demographic details of the participants involved in the empirical study.

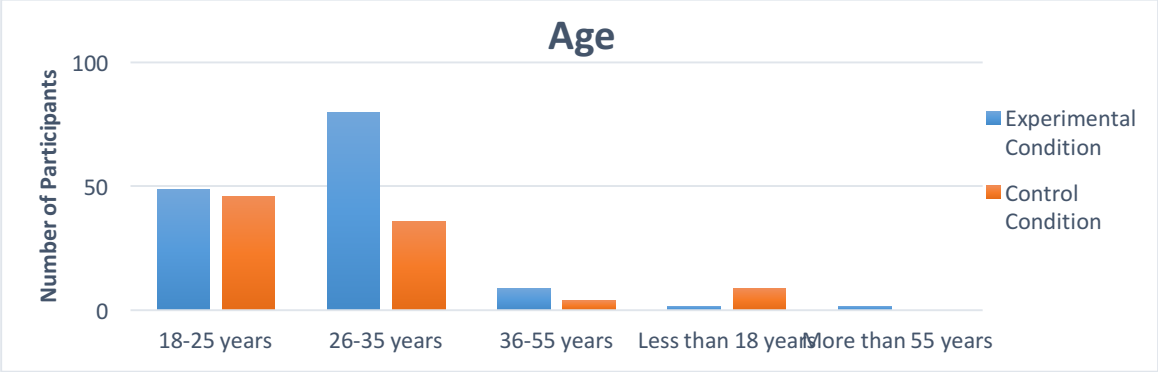


Figure 5. 1 Age profile of the participants

Number of the participants who are currently in an undergraduate programme (n = 108) and in a postgraduate programme (n=129) were close. Additionally, most of the participants did not have a background in computer science, only 19 % of all participants were from a computer science related major.

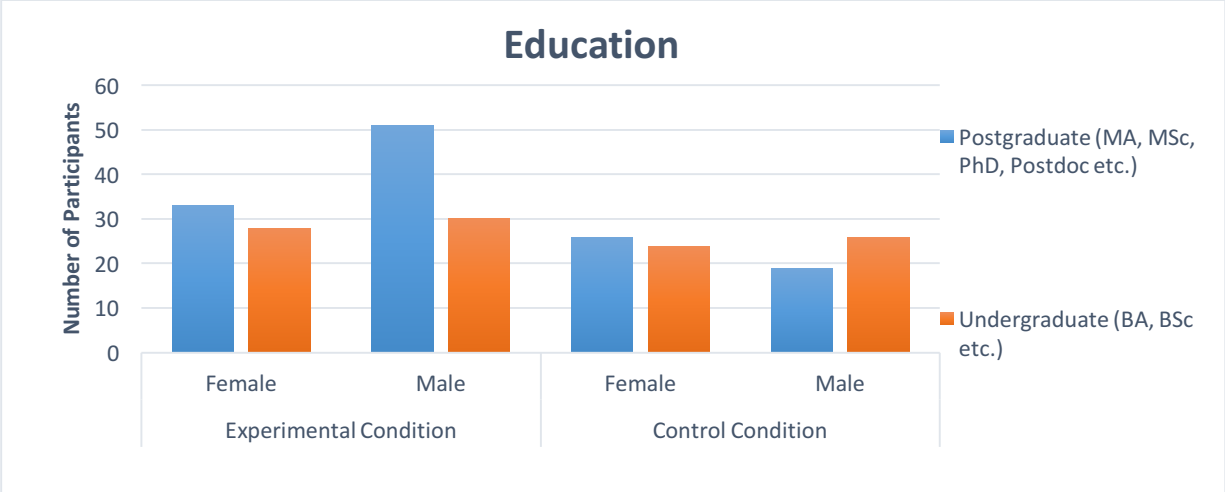


Figure 5. 2 Education level profile of the participants

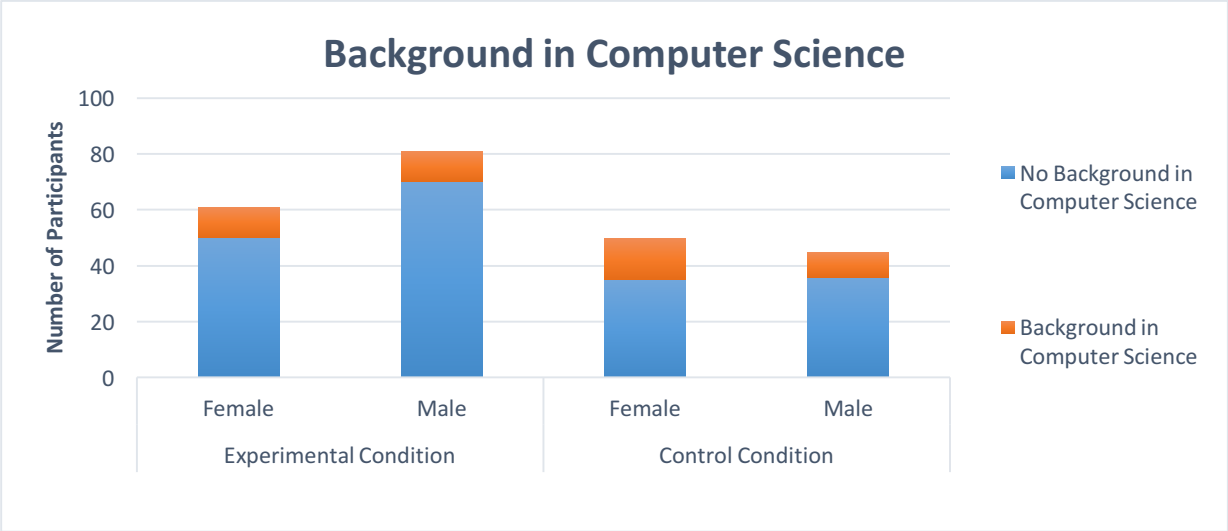


Figure 5. 3 Education background profile of the participants

This section described the design, apparatus, procedure and measurements of the empirical study and presented the full participant information. The next section presents the results and analysis of the empirical study.

5.3.3 The Results and Analysis of the Empirical Study

In the following sections, results and analysis of the empirical study are presented in detail.

5.3.3.1 The Password Analysis

Experimental and control conditions were compared in terms of password strength, password length and compliance to the common password policy rules, which were compulsory for control condition. The aim was to see whether people in experimental condition were also following those guidelines unintentionally while creating passwords in line with other methods provided. Table 5.1 presents the password analysis of the empirical study.

Table 5.1 The password characteristics

Group	Password Strength	Password Length	Password Compliance
Experimental Group	*M* =89.08 (*SD* = 8.84)	*M* = 13.39 (*SD* = 4.35)	*M* = 4.74 (*SD* = .91)
Control Group	*M* =71.95 (*SD* = 10.36)	*M* = 9.59 (*SD* = 1.80)	*M* = 6 (*SD* = 0)*

** Password compliance score was constant for control group because it was compulsory.*

**Password Strength scores were between 0-100, calculated with the Password Meter tool; Password Length is the number of the characters used, Password Compliance scores calculated as the total number of rules complied while creating a password, out of 6 rules in total.*

Password Strength:

In this study, password strength was scored out of 100 for each password individually. Though almost same number of participants in experimental and control groups think they have strong passwords (62.7 % vs. 61.1 % respectively), an independent samples t-test (t (306) = 15.617, $p < .001$, $\eta^2 = .44$) proved that there was a difference in password strength between conditions (See Figure 5.4). The experimental group (M =89.08, SD = 8.84) created stronger passwords than the control group (M =71.95, SD = 10.36). According to the Password Meter, the passwords of the control group and the experimental group are categorized respectively as *strong* and *very strong*.

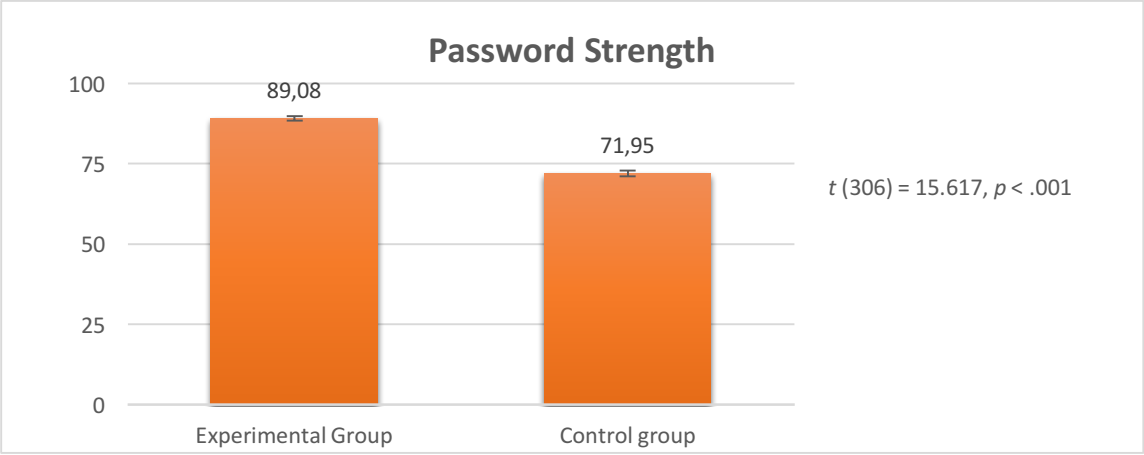


Figure 5. 4 The password strength of the experimental and control group

According to the results, people are not good at predicting the strength of their own passwords. As Figure 5.5 indicates that neither in the control group (t (93) = -1.375, p =.172), nor in the experimental group (t (140) = .034, p = .973) there were difference in terms of password strength between those who thought their passwords were hard to crack and those who thought their passwords were easy to crack.

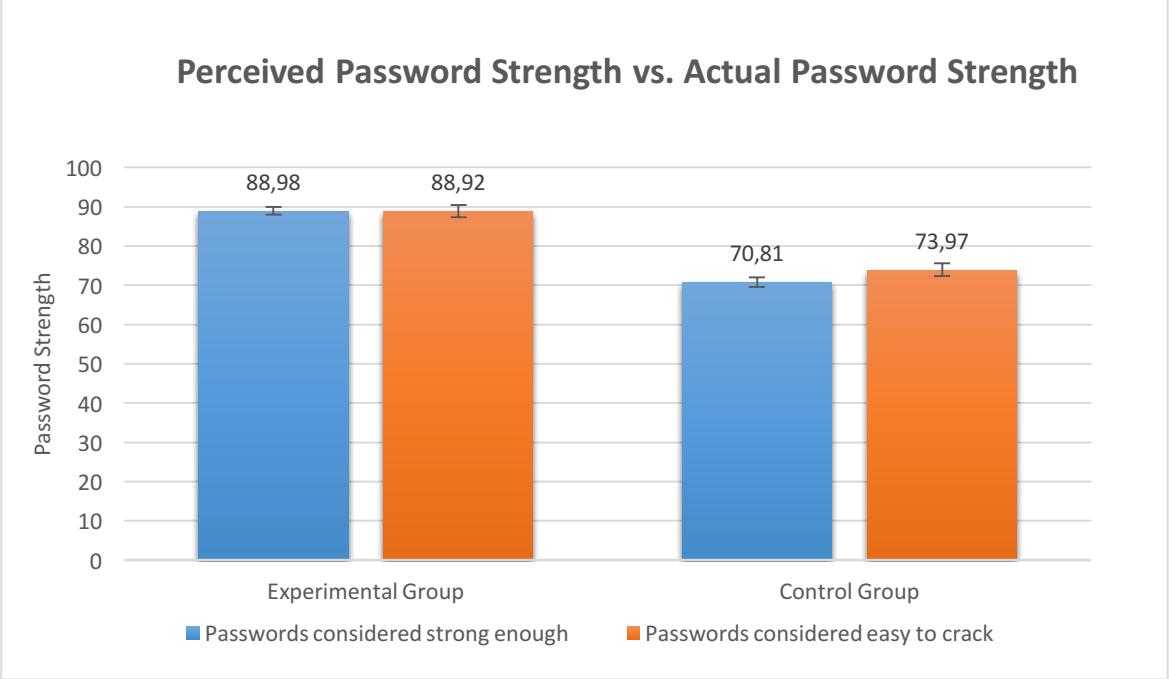


Figure 5. 5 Differences between users' perception of password strength and the actual password strength

Password Length:

Password length was also compared between groups with an independent samples t-test analysis. As illustrated in Figure 5.6, the results showed that there existed a homogeneity of variance problem, such that Levene's test for equality of variances was significant ($p < .001$). However, the t-test without equal variances assumption was also significant (t (200) = 9.986, $p < .001$, η^2 =.33). Experimental group (M = 13.39, SD = 4.35) created significantly longer passwords than control group (M = 9.59, SD = 1.80).

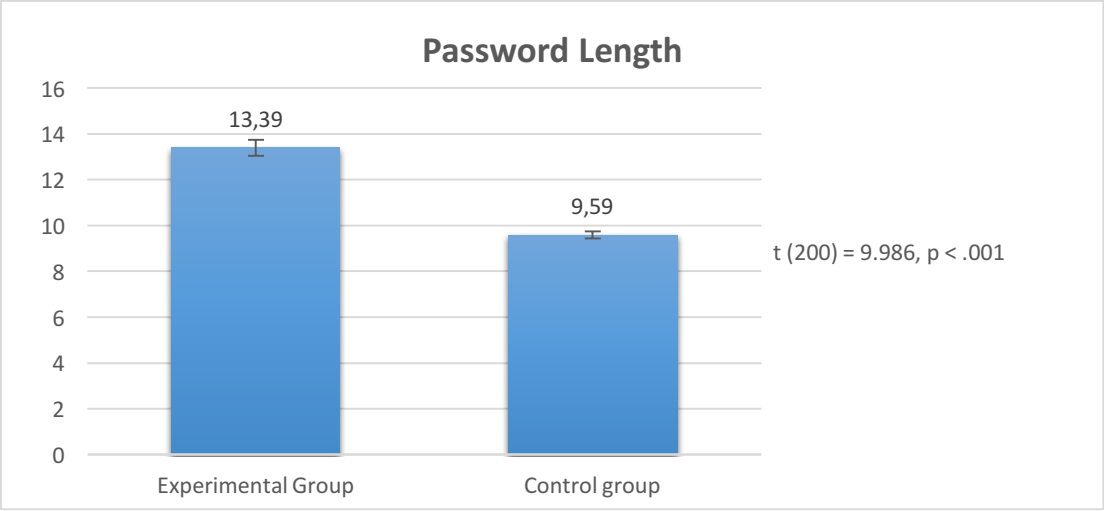


Figure 5. 6 The password lengths of the experimental and control group

Additionally, password length is correlated with password strength. A strong positive Pearson's correlation exists between them, such that the longer the passwords the stronger they are ($r = .775$, $n = 301$, $p < .001$). Figure 5.7 demonstrates the relationship of number of the characters in the password and the password strength.

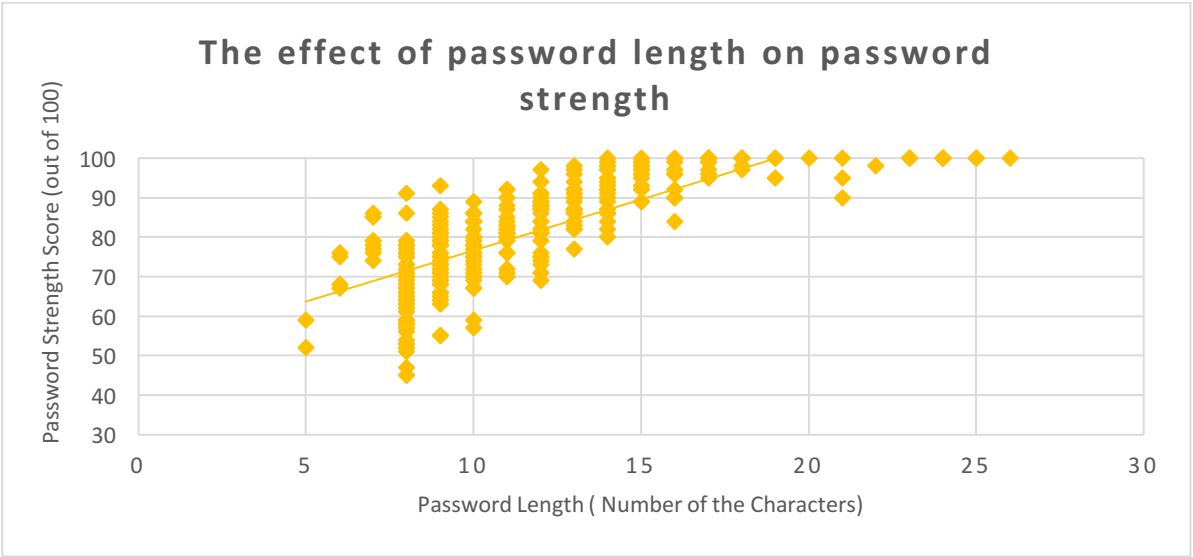


Figure 5. 7 The correlation of password strength and password length

To check for the interaction of experimental group and password length, password length scores were recoded as a categorical variable with median split method, where the length scores of both groups were divided into two groups: shorter passwords and longer passwords. Then, a 2 (experimental group) X 2 (password length) factorial ANOVA was computed. This ANOVA yielded significant results both for the password length ($F(1,304) = 166.079$, $p < .001$) and for the experimental condition ($F(1,304) = 334.695$, $p < .001$). However, there was not an interaction of the two variables ($F(1,304) = .649$, $p = .421$). Experimental group was better at creating strong passwords both for longer passwords ($M = 95.71$, $SD = 8.84$ vs. $M = 78.56$, $SD = 8.51$) and for shorter passwords ($M = 83.41$, $SD = 7.61$ vs. $M = 67.71$, $SD = 10.36$). Figure 5.8 compares the strength of short and long passwords of experimental and control group. In this analysis, there was a homogeneity of variance problem as well. However, when the analysis is repeated after data reduction based on outlier analysis with Cook's Distance values, neither the results changed, nor the homogeneity problem was solved. Since ANOVA is considered a robust test against the equal variances assumption and since the significance levels reached in the analysis were acceptable even at conservative perspective, these results were considered acceptable. Additionally, since the unequal variances are almost inevitable in this empirical design due to the difference in number of strategies given to the participants in both conditions, no data was excluded from the analyses.

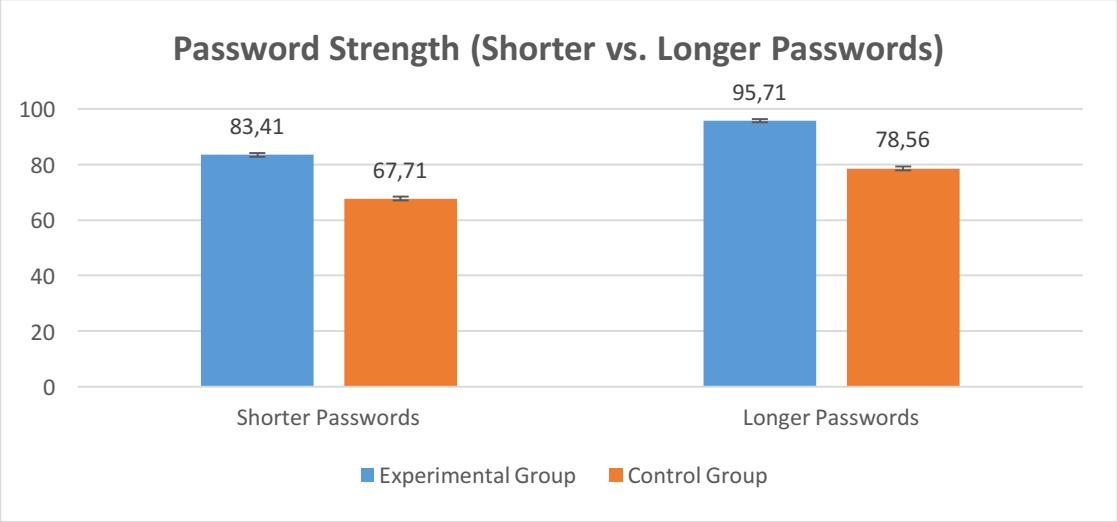


Figure 5. 8 The strength of the shorter and longer passwords of both group

Password Compliance:

At the beginning of the empirical study, the control group was required to follow a password guideline including the following password composition rules:

- The password should contain;
  1- at least 8 characters
  2- at least one upper case
  3- at least one lower case
  4- at least one numerical character
  5- at least one special keyboard character
- The password should not contain;
  6- the username

Most of the web applications require users to apply at least 4 of these rules while creating password. However, the participants in the experimental group were not imposed them to compose their passwords. Instead, their password guidelines including persuasive elements aimed at motivating users to create passwords which automatically provided these requirements.

To see whether experimental group also complied with these rules required for the control group, each password was coded in a binary format (1 for compliance and 0 for incompliance). Later, passwords were given a score as the total number of compliance across six items. Although the experimental group's compliance score was significantly different ($t(151) = -17.199$, $p < .001$) from 6, the score of the control group, still 89.5% of the participants in the experimental group complied with four or more password creation rules (see Figure 5.9).

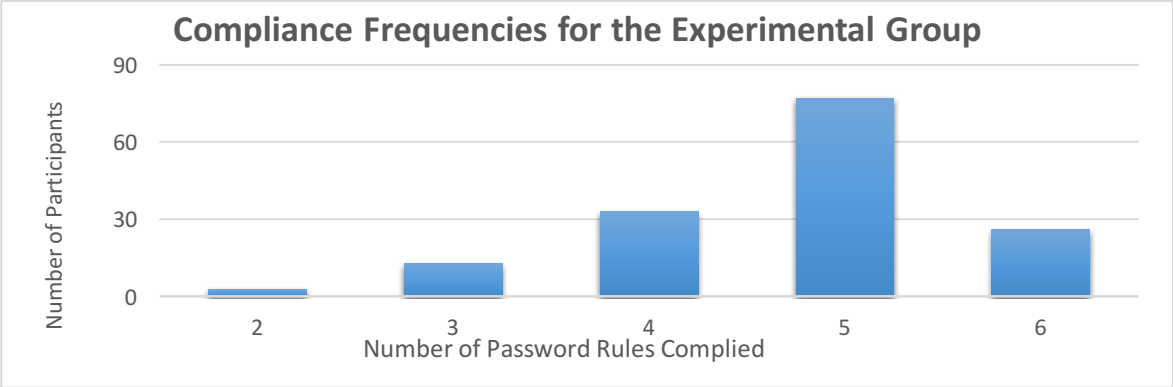


Figure 5. 9 Password policy compliance frequencies for the experimental group

The experimental group's passwords were stronger than the control group's passwords, which were obliged to comply all the strategies and therefore have the compliance score of 6. This result suggested that compliance to the commonly used password criteria was not a guarantee of strong passwords (see Figure 5.10).

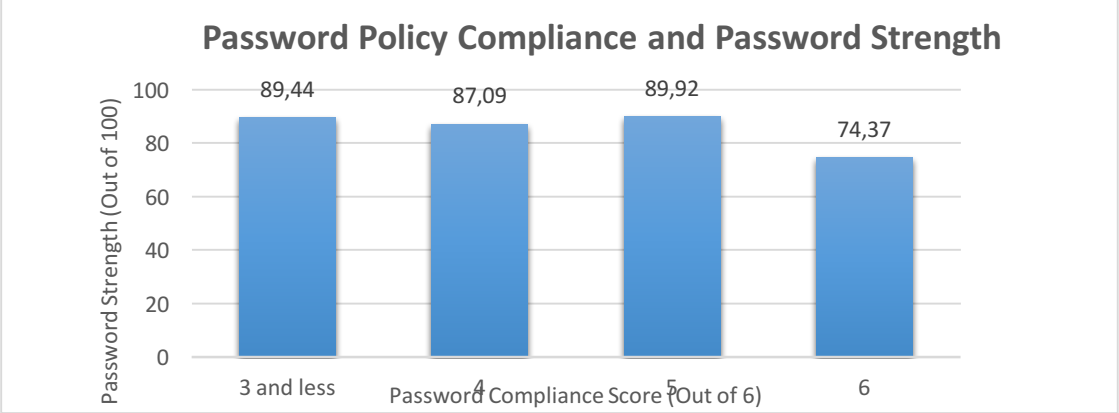


Figure 5. 10 The effect of password policy compliance score on password strength

The relationship between compliance and password strength was rather complicated. A univariate ANOVA was run to compare password strength, and the compliance scores 2 and 3 were collapsed due to the number of data in each group. So, there was a significant difference between groups $F(3,304) = 47.905$, $p < .001$. A Tukey's post hoc test showed that this difference stems from the highest compliance group, which differed from all other groups with 95% confidence intervals, shown in Table 5.2.

Table 5.2 Comparison analysis of the password policy compliance and password strength across compliance scores

Multiple Comparisons

Dependent Variable: password strength

Tukey HSD

(I) compliance	(J) compliance	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
3 or less	4	2,35	3,253	,889	-6,06	10,75
	5	-,48	2,934	,998	-8,06	7,09
	6	15,07*	2,784	,000	7,88	22,26
4	3	-2,35	3,253	,889	-10,75	6,06
	5	-2,83	2,222	,580	-8,57	2,91
	6	12,72*	2,020	,000	7,50	17,94
5	3	,48	2,934	,998	-7,09	8,06
	4	2,83	2,222	,580	-2,91	8,57
	6	15,55*	1,452	,000	11,80	19,30
6	3	-15,07*	2,784	,000	-22,26	-7,88
	4	-12,72*	2,020	,000	-17,94	-7,50
	5	-15,55*	1,452	,000	-19,30	-11,80

Based on observed means.

The error term is Mean Square(Error) = 114,028.

*. The mean difference is significant at the ,05 level.

Memorability:

How likely people were to remember a password they create is another central point. In this study, first, memorability of a password after a week and after a month were compared across groups with a 2 (time: week vs. month memorability) X 2 (experimental group) factorial ANOVA. As shown in Figure 5.11, results indicated that memorability significantly decreases as time passes ($F(1,306) = 59.712$, $p < .001$). Memorability after a week ($M = 1.31$, $SD = .83$) was significantly higher than memorability after a month ($M = .85$, $SD = .81$), where a score of 2 indicates correctly remembering a password at first trial, score of 1 indicates correct remembering at many trials, and a score of 0 indicates failing to remember. Additionally, the chances of correct retrieval were higher for experimental group ($M = 1.27$, $SD = .05$) than the control group ($M = .90$, $SD = .05$; $F(1,306) = 28.320$, $p < .001$). This result is in line with experimental group's predictions about memorability, where 86 % of participants thought they would remember the password correctly after a week, and 76% of them thought they would remember correctly after a month (see Figure 5.12). Hence, no interaction between experimental group and time was found ($F(1,306) = .425$, $p = .515$).

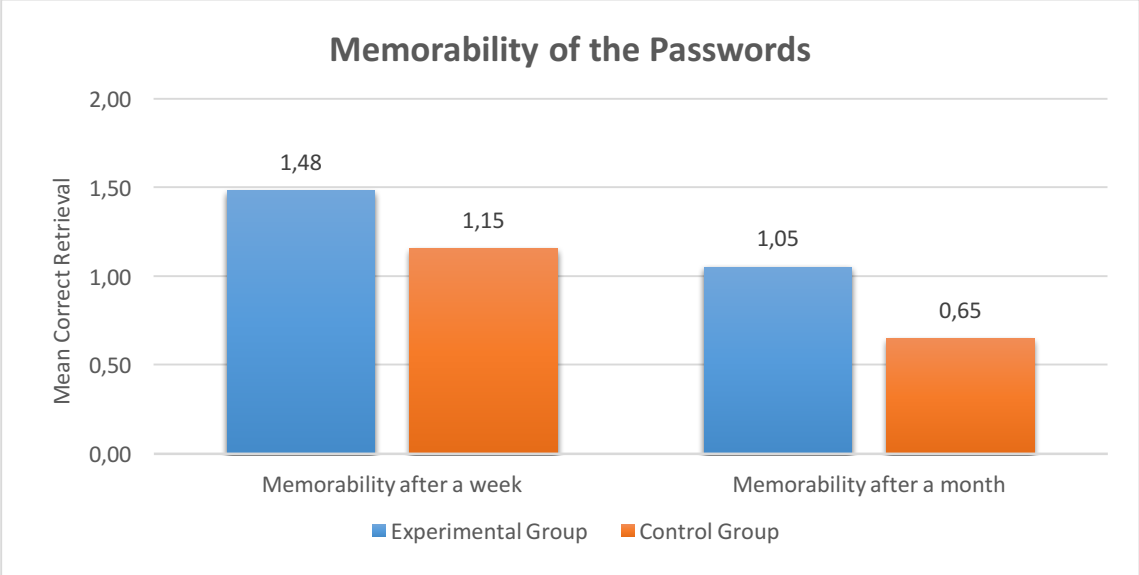


Figure 5. 11 Memorability of the passwords of experimental and control group

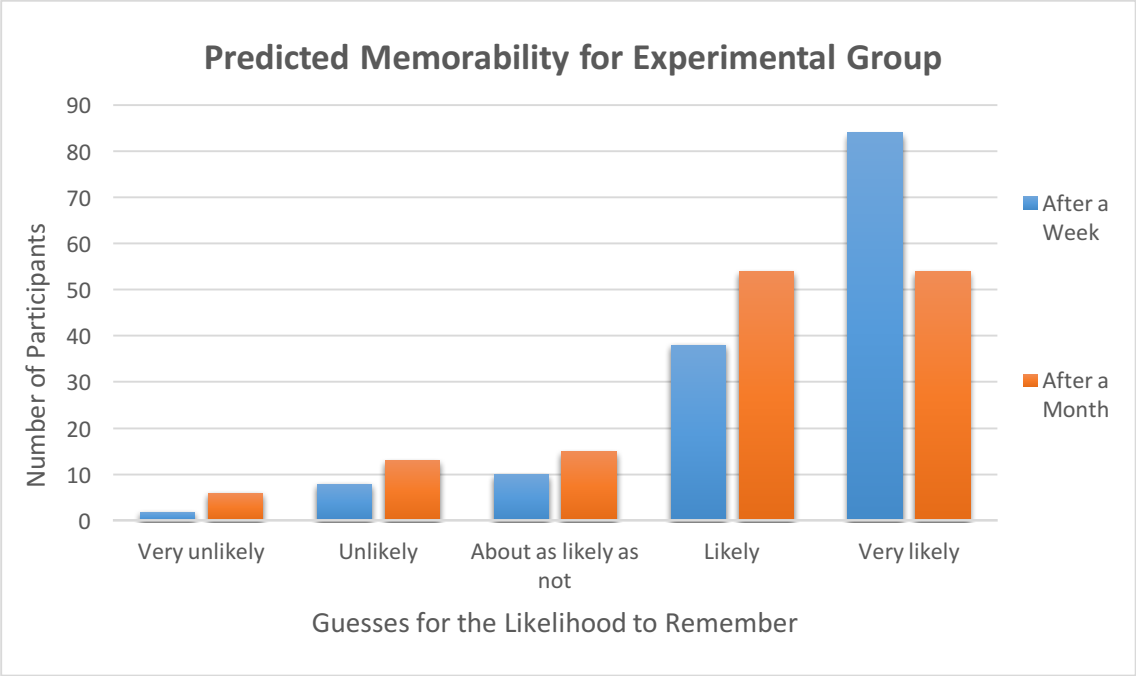


Figure 5. 12 Users' predictions of memorability in the experimental group

To investigate how the conditions were distributed across retrieval levels, two chi-square analyses were run. For the memorability of a week, the chi-square test was significant, χ^2 (1, N = 308) = 15.487, p < .001, which meant that experimental group and control group differed from each other at retrieval performances (see Figure 5.13). Grouped comparisons supported that the significance stemmed from differences at all levels. In a week period, the experimental group was better at both correct retrieval at first trial (101 vs. 69 participants) whereas the control group either failed to remember more than the experimental group (28 vs. 45) or retrieved correctly at many trials with higher frequency (23 vs. 42).

The second chi-square analysis showed that the experimental group (57 vs. 25 participants) again performed better at correct retrieval at first trial, χ^2 (1, N = 308) = 20.147, p < .001. Similarly, the control group failed more to remember their passwords correctly (49 vs.80 participants) after a month.

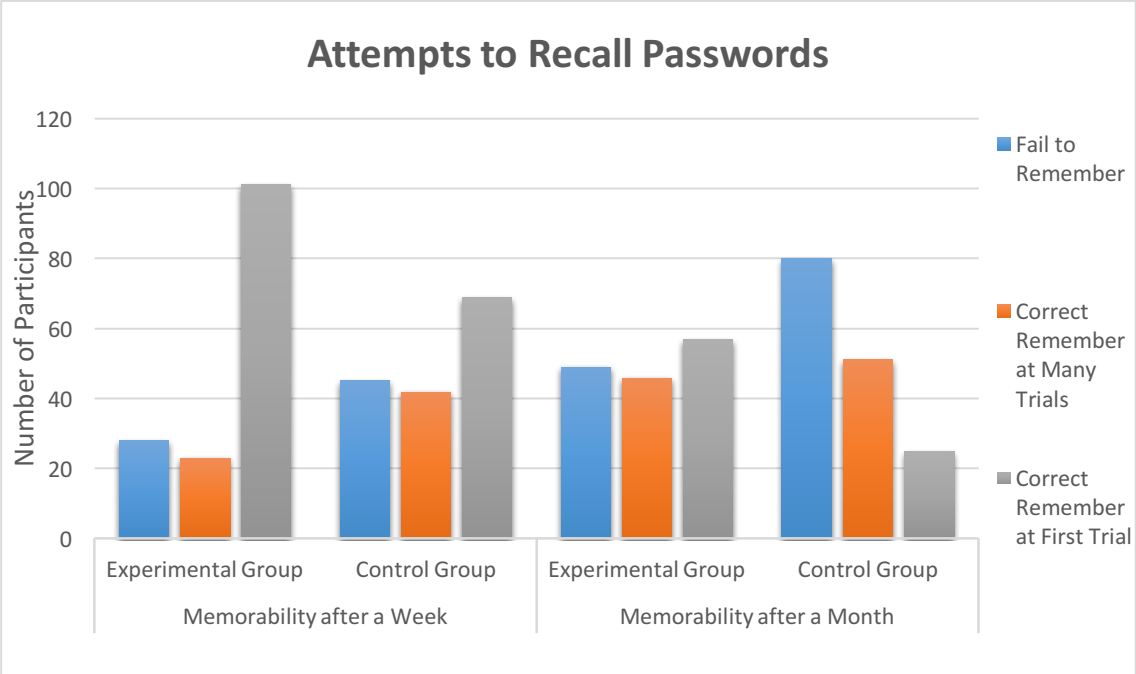


Figure 5. 13 Attempts to recall passwords after a week and after a month

Use of Password Creation Methods in the Experimental Group:

Among the 142 participants who took the follow up questionnaire, 3 participants were excluded from the following analyses since they selected more than one option at the same time. Among the remaining participants in the experimental group, most of them preferred the third method (34 %) (see section 5.3.2.1 for the details of the given methods). Distribution can be seen in Figure 5.14.

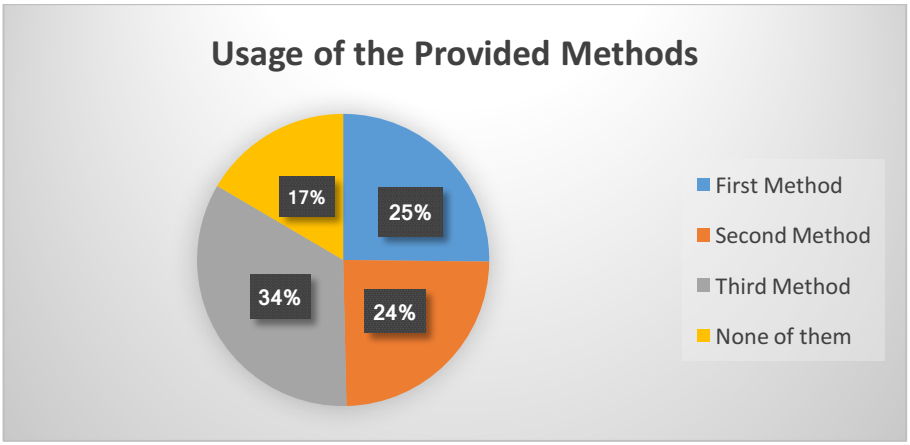


Figure 5. 14 Preferences for the given methods in percentages

Moreover, password creation methods were compared in terms of how strong passwords the participants created by applying these methods (see Figure 5.15). A univariate ANOVA showed that passwords created by different methods were significantly different, $F(3,135) = 30.097$, $p < .001$.

To understand which methods are creating the difference, a Tukey's HSD post hoc test was run, and resulted that the passwords created by applying any of the methods are stronger than the passwords created without applying the given methods (stated as none of them in the figures), with 95 % confidence interval (see Table 5.3). Additionally, passwords created with the method three were slightly stronger than the passwords created with the method two ($p = .047$).

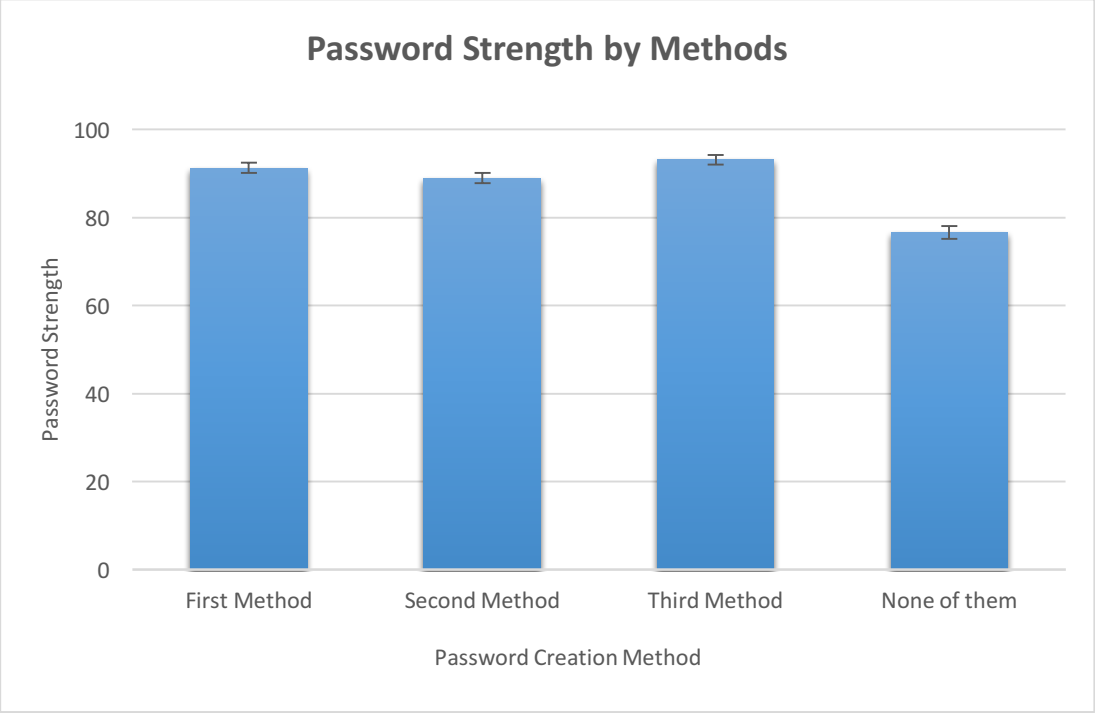


Figure 5. 15 Password strength by methods

Table 5.3 Comparison analysis of the password strength among the given methods

Multiple Comparisons

Dependent Variable: password strength

Tukey HSD

(I) methoduse	(J) methoduse	Mean Difference (I-J)	Std. Error	Sig.	95% Confidence Interval	
					Lower Bound	Upper Bound
First Method	Second Method	2,32	1,700	,525	-2,11	6,74
	Third Method	-1,86	1,576	,639	-5,96	2,24
	None of them	14,63*	1,895	,000	9,71	19,56
Second Method	First Method	-2,32	1,700	,525	-6,74	2,11
	Third Method	-4,18*	1,589	,047	-8,31	-,04
	None of them	12,32*	1,906	,000	7,36	17,28
Third Method	First Method	1,86	1,576	,639	-2,24	5,96
	Second Method	4,18*	1,589	,047	,04	8,31
	None of them	16,50*	1,796	,000	11,82	21,17
None of them	First Method	-14,63*	1,895	,000	-19,56	-9,71
	Second Method	-12,32*	1,906	,000	-17,28	-7,36
	Third Method	-16,50*	1,796	,000	-21,17	-11,82

Based on observed means.

The error term is Mean Square(Error) = 49,817.

*. The mean difference is significant at the ,05 level.

Password Cracking Times:

To measure the strength of the passwords in the experimental and control group in another way, a tool namely *"How Secure is My Password"* was also used. This tool measures the estimated cracking time of the created passwords.

When the passwords were analysed based on the time required to crack them, data indicated that only control group participants and the participants in the experimental group who did not utilize any of the given methods created passwords which are easier to crack (i.e. passwords which could be broken in less than a year). Additionally, when the experimental methods were compared to each other, most of the participants who used method two created passwords to be cracked in decades, as opposed to the participants who preferred the first or the third method. This result is in line with password strength results, which indicated method two created slightly less strong passwords than methods one and three. Estimated password cracking times for both groups' passwords are shown in Figure 5.16.

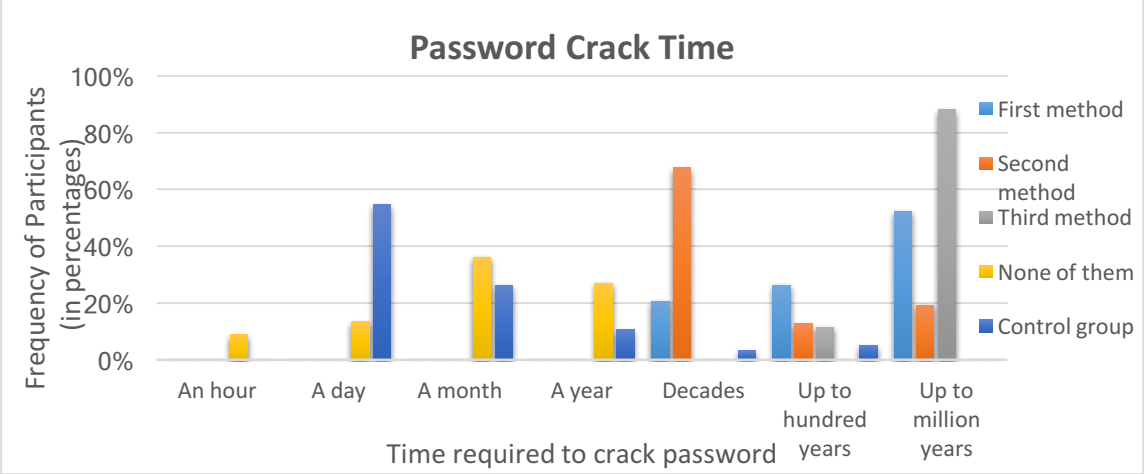


Figure 5. 16 Estimated password cracking times

5.3.3.2 The Results Based on the Survey Responses

Password Usage:

Among the participants who conducted the questionnaire, 80.3 % of the experimental group and 66.3 % of the control group reported that they did not experience

any password security failure before. Moreover, only 39.4 % of the experimental group and 31.6 % of the control group reported that they do not write down their passwords anywhere while 41.5 % of the experimental group and 38.9 % of the control group write their passwords somewhere safe and 19 % of the experimental group and 29.5 % of the control group prefer somewhere accessible.

Results also showed users' password preferences across different accounts vary. As seen in the Figure 5.17 most of the users tend to choose stronger passwords for their personal email accounts than the work emails.

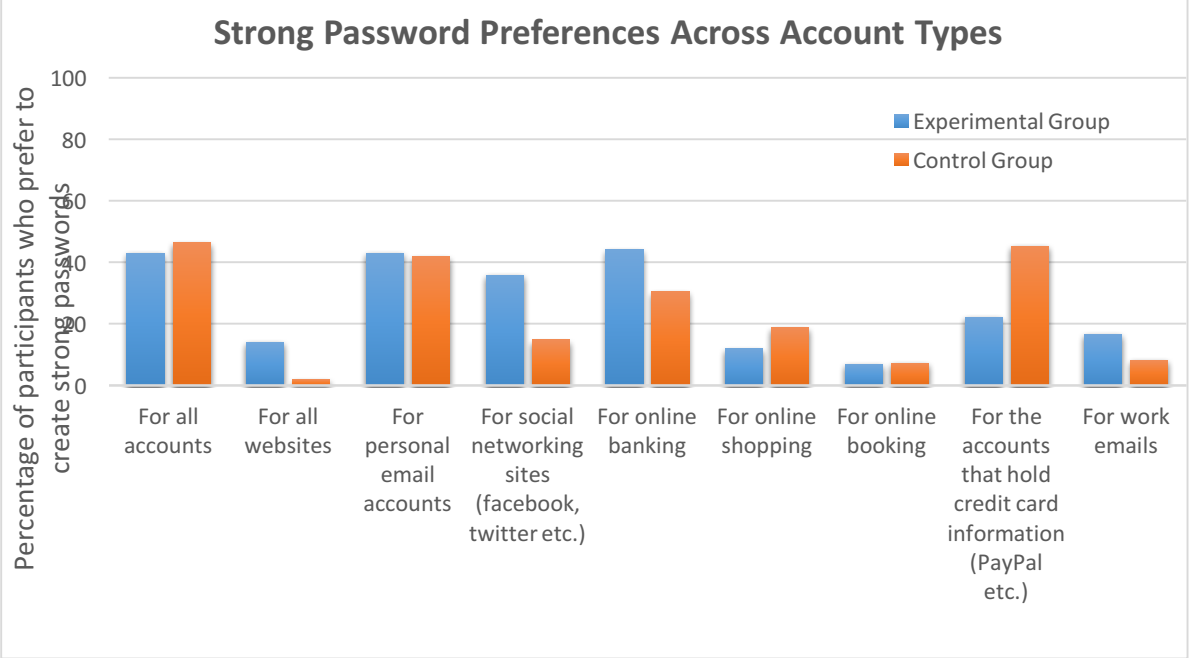


Figure 5. 17 Users' password preferences across different accounts

User Satisfaction:

Participants in the experimental group were asked about their experience of using the new methods presented to them. As illustrated in Figure 5.18, most of the participants reported that they found the given methods useful to create a password for the current empirical study (87%) and they were likely to use given methods to create passwords in the future (79 %).

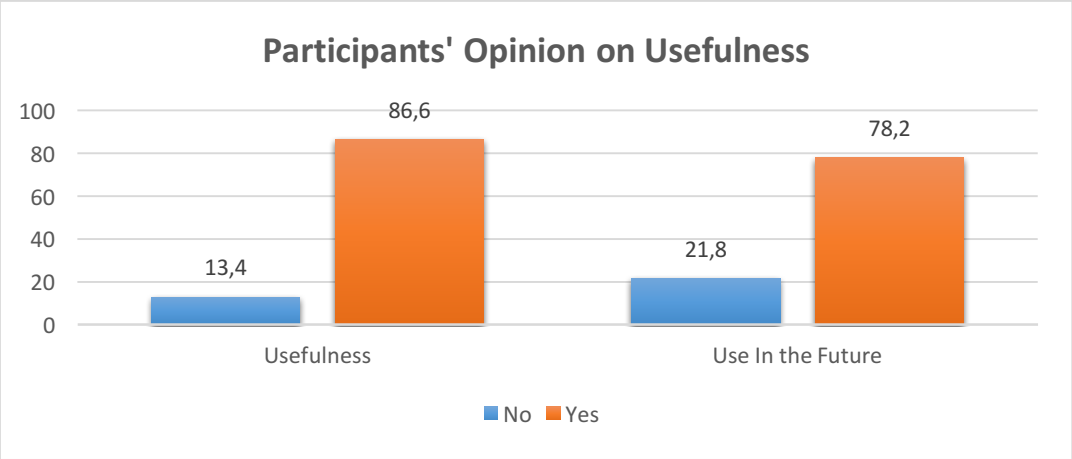


Figure 5. 18 Participants' opinion about the usability of the given methods

Additionally, they rated their experience further in terms of fun and easiness. Most of the participants agreed that using the provided methods was easy (61%) and more than half of the participants evaluated the methods as fun to apply (54 %). A larger body of participants (80%) reported that using the given methods to create secure passwords are worth the time spent on them. Moreover, most of the participants (85 %) agreed that these methods were more efficient than the commonly used strict password creating rules, in terms of creating strong and memorable passwords (see Figure 5.19).

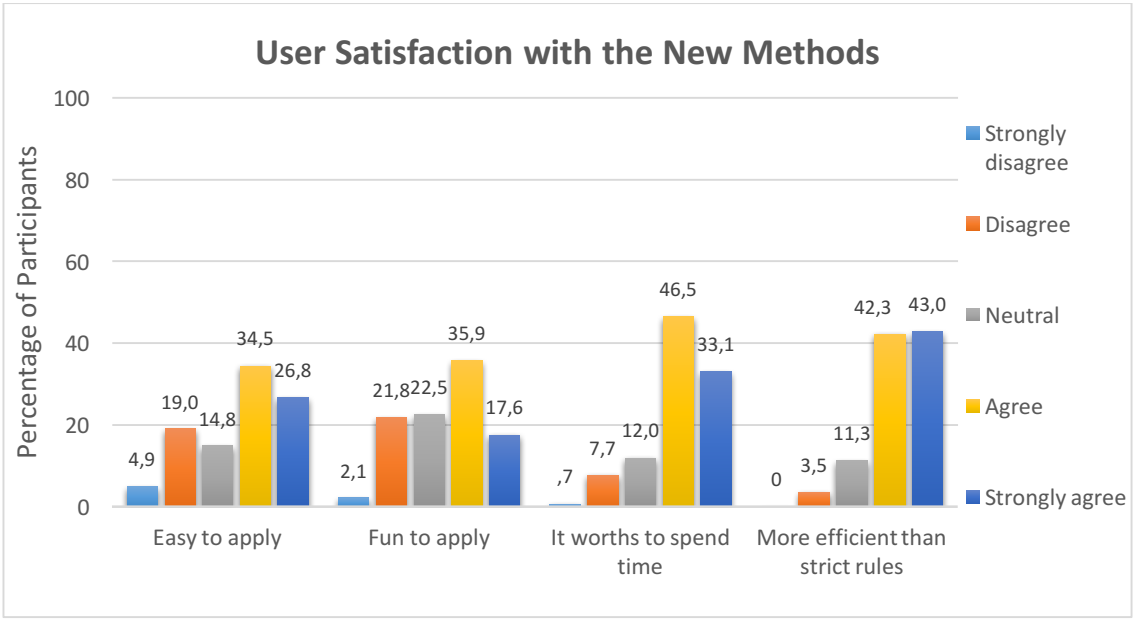


Figure 5. 19 User satisfaction with the new methods

Persuasiveness:

Finally, it seemed like the methods provided to the experimental group persuaded them not to use any of the coping strategies (see Figure 5.20). Most of them reported they would not write down their passwords (76 %); not share their passwords with other people (75 %) and not reuse the passwords they created once (73 %).

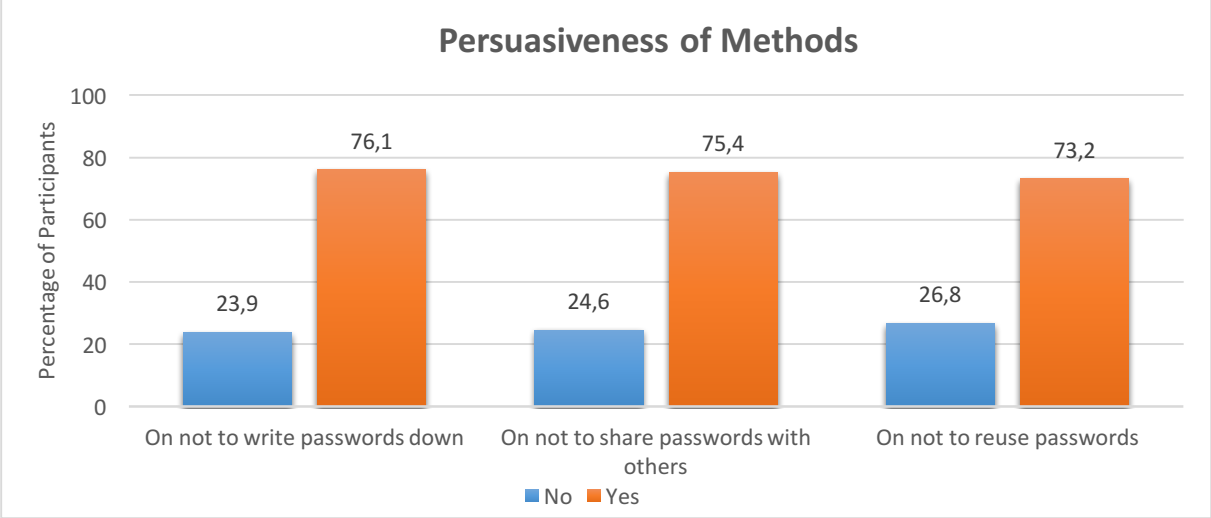


Figure 5. 20 The given methods' persuasiveness to abandon coping strategies

5.4 DISCUSSION

The details of the web-based empirical study are presented in the previous sections. As stated at the beginning, the aim of this study was investigating whether users can create stronger and more memorable passwords if they are not enforced to comply with strict password policy rules. The study examined the efficiency of a persuasive text along with the three password composition methods on motivating users to create stronger and memorable passwords.

The results indicate that passwords created by users who receive password guidelines including a persuasive text and sample password creation methods are stronger compared to passwords created by those who are given the password guidelines including strict password composition rules. The results also showed that the participants who applied the given methods, remembered their passwords better than the ones who

followed the usual password policy rules.

Thus, these findings suggest that it is a good idea for providing a message in the password guideline to persuade users to create their own password composition formula. When the message is supported with the example methods of password composition, it becomes possible to create strong passwords without burdening their memory to remember them. In this study, most of the participants in the experimental group spent time to read the information and applied the given methods to produce passwords, maybe just to help a research study by participating. However, in real life, users may not make an effort to read the information provided in the password guidelines unless they have to. Zakaria (2013) suggested that one possible way to overcome this is to make reading and understanding the password guidelines compulsory before constructing a password. Especially if the systems or applications require a high level of password security, this might be a reasonable solution. Another solution is visualization of password attacks in password guideline to make users aware of the threats (Zhang-Kennedy, Chiasson and Biddle, 2013). Ur et al. (2015) stated that password advice should focus on promoting human algorithms for developing passwords, in addition to visualizing threats in the password guideline. Some researchers claimed that users should be guided to save their limited mental capacity for passwords for high-value accounts (Florencio, Herley and van Oorschot, 2014; Nithyanand and Johnson, 2013; Ur et al., 2015).

The methods given in the password guideline of the experimental group allowed users to create passwords which spontaneously meet the requirements of the password policy which was given to the control group as password guideline. In other words, most of the participants created passwords which are longer than 8 characters, including upper-lower cases also numbers and special keyboard characters. However, the study showed that complying with these rules does not always guarantee creating strong passwords.

There are more attributes such as password length and not including meaningful words in passwords that affect the password strength. Therefore, two tools were used to measure password strength considering the frequency and variety of characters as well as the similarity to the dictionary words. Although, the results of the measurements performed with the *Password Meter* showed that the control group's passwords are less strong then the experimental group's, they were still in the 'strong' category. However, the difference between the cracking times measured with the "How Secure is my

Password" is huge. Most of the passwords of the control group categorized as strong seemed likely to be cracked in a day. The reason of this difference is that the second tool takes into consideration whether the password looks like a dictionary word besides measuring the character variability. The passwords including meaningful details such as dictionary words are likely to crack in short times even if they are composed of different characters. As a result, both measurement yielded results in support of password guideline including persuasive message and the example password creation methods.

Furthermore, questionnaire responses showed that the given methods are efficient to persuade users to abandon coping strategies to remember their passwords. Users in the experimental group seemed to be willing to comply with the password guideline and apply the given methods. However, a little more than half of the participants (54 %) found the methods fun to apply. To increase the user satisfaction and lessen more the memory burden, images can be included in the password creation process.

There is lack of ecological validity in generalising the findings to real life as the study is not conducted with a real application in use. The participants knew that the websites created for a research study and they created passwords for helping the study. If users created passwords for a real website to perform their own tasks, quality of the passwords and compliance with the guidelines might have been different. On the other hand, the password guideline including several password creation tips provided to the experimental group is somewhat long to read. Therefore, users might not be willing to read it when they create a password in real life. This reduces the practicability of the proposed guideline. Another issue about the study is the unusual demographics of the experimental group. The participants were randomly assigned to the experimental and control groups. However, number of the participants who have high education level in the experimental group is more than the control group. This situation might have affected the password strength rates in the experimental group.

Thus far, the results generally have shown some promising findings; however, the practicability of this new password guideline may be an issue in real world, as stated above. The password guideline can be improved adding visual elements in the guideline to make reading the given information process interesting. Further discussion and suggestions can be found in the conclusion chapter.

5.5 SUMMARY

A web-based empirical study conducted to evaluate the effectiveness of the proposed password guideline including a persuasive message and several password creation methods on password strength and memorability is presented in this chapter. A follow up questionnaire was also conducted to investigate users' password creation habits, persuasiveness of the given methods, and the user satisfaction. Several measurements have been performed to evaluate the efficiency of the proposed password guideline, and the results and findings have been discussed in the chapter.

The password guideline study provided the opportunity to see the effect of password policy rules on users' password choices and compare it with alternative password creation methods set as examples for users to create better passwords.

While motivating users to create their own strategy to compose passwords by the proposed guideline yielded good results regarding password strength and memorability, the password creation process should be easier and more enjoyable for users. The participants who have been persuaded to create their own password creation formula to turn simple words to complex passwords may still have difficulties to remember their passwords and even their formula as days move on. To find a better remedy for remembering complex passwords to lessen the memory burden, and to avoid a dull password creation process, new solutions are required.

Therefore, the next part of the thesis focuses on the other form of knowledge based authentication: graphical passwords. As human memory is better at remembering images than texts, graphical passwords can be included in the authentication systems. The graphical passwords are promising alternatives to textual passwords as they are relatively easy to use and cheap to implement compared to biometrics and tokens. However, they don't seem likely to replace the text passwords everywhere since most of the systems still use the traditional text-based password authentication. Therefore, including images with the text-based password authentication mechanism as an assistance tool for users to remind their passwords might be a good idea. In recent years, especially, many authentication schemes integrating text and graphical passwords have been proposed.

In the following chapter review of the alternative authentication systems by specifically focusing on graphical passwords will be presented.

CHAPTER 6

REVIEW OF THE USER AUTHENTICATION MECHANISMS

6.1 INTRODUCTION

As computer technology has become more essential for everybody day by day, providing safe and secure ways to authenticate users to access confidential information or networks on different systems becomes increasingly important too. As authentication is a requirement for almost all IT systems today, its reliability is significant for computer and information security. While most of these systems require a classical password to give access to users, some of them use hardware e.g. tokens or users' biometric information for authentication. Before such development of computer technology, a simple password was sufficient for verifying someone who claims to be the right person to access privileged information and resources. However, in time, as the computers' computation power increased significantly, brute force attacks became possible in a short period. Therefore, developing more secure systems is necessary.

As users have to authenticate themselves on many systems which require a password or PIN they encounter some difficulties to remember such information. The fact that the passwords should be complicated enough to resist hacker attacks make memorizing even harder. This situation generally results with users' bad password practices such as choosing poor passwords or writing them down. Thus, these passwords become vulnerable to social engineering and brute force attacks. To make the authentication process easier and more secure, several novel authentication systems have been created or the existing approaches improved by researchers in the past few decades. However, these alternatives still have their own shortcomings.

One of the past few research papers about secure authentication by Morris and Thompson (1979) described a design of the password security scheme on a timesharing system which is accessible remotely. Their design was for countering attempts to penetrate the system. They presented the password algorithm and invited attack instead of attempting to hide the security aspects of the operating system. They suggested that a time-sharing system must perform in a hostile environment believing that this approach would minimize the troubles. However, that design was a compromise between security

and ease of use. Brostoff (2004) in his PhD thesis reconceptualised how to create memorable but secure passwords as how to improve password system effectiveness. He modelled password system performance by using Reason's (1990) Generic Error Modelling System (GEMS) as a basis (Brostoff, 2004).

In this chapter, existing authentication methods have been reviewed and their upsides and shortcomings presented. The main reason of this review is to find out whether a good alternative authentication method(s) to replace traditional text-based password exists. Also, this chapter aims to determine the most effective authentication system by comparing all the alternative mechanisms based on security and usability criteria.

6.2 EXISTING AUTHENTICATION MECHANISMS

The goal of authentication mechanisms is ensuring the data is to be transmitted to the person who is supposed to receive the data without being lost and modified. The data should also be confidential between the sender and receiver. For confidentiality, the efficiency of the authentication mechanism is important. If the data is sent to others than the target person it might cause pecuniary loss and intangible damages. To avoid this, many researchers who are aware of the serious security problems of the authentication systems, developed a wealth of different methods. However, none of these methods are currently perfect and problem free.

This section focuses on a broad overview of the available alternatives in authentication systems. These alternatives will be discussed considering their implementation as well as their advantages and disadvantages. So, the overview presented here will provide a general understanding of the existing alternatives which allows this thesis to focus on the best alternative(s) to elaborate the research future.

A classification schema was proposed by Renaud (Renaud, 2003) and used by some researchers (Yampolskiy and Govindaraju, 2006; Yampolskiy, 2007) to categorize the alternative mechanisms. Renaud, in her paper, considered the location of users as one of the possible approaches while determining the quality of authentication mechanisms contrary to other researchers. However, users' location information was still thought as a questionable way of authenticating (Renaud, 2003). According to the aforementioned schema, the authentication approaches can be categorized under four sections which

depend on what the user has, who the user is, where the user is located and finally what the user knows. There are also some multifactor authentication schemes which use combinations of two or three authentication methods.

6.2.1 Token-Based Authentication

This authentication approach is based on the idea of using a physical token which should be hard to obtain or falsify. There are a few alternative devices that users can use.

6.2.1.1 Memory Cards

Memory cards are the first possession based authentication alternative which has a magnetic strip which holds user information within and relies on a reader in order to process the information. The authentication basically requires users to insert their cards into the reader and then enter a set of credentials. ATM (automated teller machine) card is one of the most commonly used memory cards. It works when the user pops the card in the ATM machine and then enters his PIN number. The card supplies the private user information and then the user enters the secret code (PIN), together providing a credential set (Zakaria, 2013). Also within many companies, employees will often carry ID cards which is mostly a PIN hashed and stored on the magnetic strip on the cards. Employees must enter a PIN number and swipe the card through a reader when they enter the company building. The reader hashes the entered PIN number and compares it to the value on the card itself. If they match, the access is granted.

The advantages of using memory cards is that it can be carried everywhere easily as its size is small enough to fit into most wallets. Although the size is small, it has large data storage capacity which works easily and fast. Also, it is quite cheap compared to other similar alternatives. However, the main drawbacks of it is that it can easily get corrupted and cause the loss of data so it should be handled carefully.

6.2.1.2 Smart Cards

Another quite similar alternative is the smart card which is a version of memory card by its ability to process information as it has a microprocessor and integrated circuits.

When the user inserts the smart card into a reader which has electrical contacts that interface and activate the smart card processor. The user will then enter a PIN value which gives access to the information within the smart cards. A smart card could be worked in different ways such as holding user's private key, generate a onetime password or respond to a challenge-response request.

The advantages of smart cards are being much more secure when compared to memory cards as they can lock themselves if several false PIN are entered. In this case, it would require the user to contact the vendor to receive a new PIN value to unlock the card again. The downside that both smart cards and memory cards have is the extra expenses of creating new cards and purchasing the required readers which must be included in their implementation and lifetime costs (Chadwick, 1999).

6.2.1.3 Security Tokens

A token device is usually associated with one-time passwords which is generated and supplied to a user by the system itself. These passwords can be used to prove a user's identity once only. After the password is used, it is destroyed and not accepted for authentication any longer. If the attacker somehow manages to obtain the password during transmission, he would have a limited time to try and use it, and most probably it was already used once thus rendered useless to the attacker. This is one of the advantages of one-time passwords used in token devices which significantly reduces the chance of success of someone sniffing network traffic to obtain passwords and trying to authenticate him as an actual legitimate user. Also, password guessing, replay attacks and electronic eavesdropping can be eliminated by token devices.

Nevertheless, the drawback of token devices is that they can be exposed to masquerading attacks. This means an attacker might gain control of the token device and use it to impersonate the actual user. This is the reason for which many token devices require the user to enter a proper PIN value before it is used.

6.2.2 Biometrics-Based Authentication

Biometrics-based authentication is one of the promising alternatives which take the advantage of the uniqueness of details in a person's anatomy or behaviour to prove that the person is the one who is supposed to be. Fingerprints, retinal patterns, signatures, iris scans, keystroke dynamics and voice properties are some examples of unique personal attributes which can be used to verify a user's identity. If the anatomic or behavioural characteristics of a user match the electronic equivalent of those characteristics recorded in the computer, it is accepted as valid.

Within biometric systems, the user has to go through an enrolment period first. During this period, personal attributes are captured and stored in a file to be held in a database or a biometric template of a smart card. This enables a user to input his identical information (e.g. finger print) onto the reader in order to access the system. If the image matched the one in the database, the user will be successfully authenticated and allowed to enter the system.

The uniqueness of biometric systems is that it gathers a lot of personal information which is hard to imitate, so they provide a higher level of security compared to other authentication technologies. However, biometric systems are usually more expensive than other mechanisms and are not usually adopted by society since it is perceived as an intrusion of one's personal information. Moreover, biometrics are generally associated with usability problems. For example, because of a sensitive and time consuming process through the enrolment phase, users might have difficulties to stay calm in such a controlled environment (Briggs and Olivier, 2008).

6.2.3 Knowledge-Based Authentication

This is the most popular approach to authenticate users based on what a user knows to prove his identity. Within knowledge based authentication scheme, users and system administrators have some confidential information such as passwords, usernames and answers to secret questions. If this information revealed by the users to prove his authenticity matches the information in the system's database, the system administrator is able to verify the user's identity and allows him to access the system.

The aim of knowledge-based authentication (KBA) is to find a balance between privacy, security and usability. While it is also called "secret questions," KBA is often used as a backup or retrieval system for users who forgot their passwords. When a user forgets his password, he can get in contact with a KBA system. The system prompts the user for the answer to a secret question which could be selected and answered by the user previously (static) or asked by the system itself by gathering data in the public records (dynamic). In static schemes, if the question is answered correctly, the system either retrieves or resets the password. This can be done through a link on a web site, or over the phone through a customer service or help desk representative. Users often set up the answers to their secret questions at the same time as their user ID and password. After a while, when they are asked to answer a secret question, they generally forget the secret answer which defeats the whole point of KBA. Briefly, both static and dynamic schemes rely on the given answers to the secret questions. If the answer is correct then the respondent's identity is confirmed.

The problem with static KBA questions is that if the user in some way shared his private information e.g. on a social media site, the answer can be easily guessed. Although the answers to dynamic questions could be searched, it would take a long time which is not given to the answerer. If the respondent does not answer the dynamic question within a certain time, the question is discarded and treated as a wrong answer. The dynamic scheme still has security flaws just as the static scheme has. While the security of 'shared secrets' (static KBA) is a very important issue for computer systems, it is beyond the scope of this study. Within this study, specifically security and memorability of passwords will be focused on.

The knowledge based authentication mechanisms can be divided into two main classes: Text based Passwords and Graphical Passwords.

6.2.3.1 Text-Based Passwords

Text based password authentication is the most commonly used authentication mechanism in computer systems. It basically requires creating and then using a password

which is an array consisted of keyboard characters for authentication. Either this password can be created by the user himself or chosen by the system automatically.

Text based approach can be subdivided into three groups which are syntactic, semantic and one-time methods. Within all these methods, the password is basically a string of keyboard characters. The difference between them is the way the string is created.

Traditional text based passwords and passphrases are the example of the *syntactic* method in which a user is expected to recall a sequence of keyboard characters or words which was created before. The sequence can be composed of characters in only one of the groups of letters, numbers or signs as well as combination of the characters in several groups such as "John", "John78" or "John78!". However, for most of the systems, the initial of the password must be a letter. Syntactic passwords can be produced by the user himself or generated for him by the system (Renaud, 2003). The main disadvantage of this method is that in most cases, users' information can be attained by unauthorized people easily. This is because the users tend to share their passwords or make them available for others. The fact that users' ability to remember complicated passwords is limited and, multiple passwords for different accounts make it even harder for them. In this case, authentication may cause problems for users. Alternatively, easy to remember passwords are generally predictable so they decrease the level of security.

Actually, users are aware of the importance of the password security since most of them are frustrated by their experiences with traditional passwords (Dhamija and Perrig, 2000). Even if they want to behave in a secure manner, they often do not comprehend what constitutes a "secure" password since the guidelines for the creation of secure passwords are generally inadequate (Weir et al., 2010). Even with good password policies in use, users will prefer to choose the path of least resistance e.g. choosing simple passwords, storing them in plain text on their mobile devices or using the same password for different accounts because of human nature (Adams and Sasse, 1999; Bes-Asher et al., 2011). According to findings of Ives, Walsh and Schneider (2004) this is understandable since even an ordinary user is expected to recall an average of 15 different passwords on a daily basis. Due to limitation of human memory, users can normally handle maximum four or five passwords (Adams and Sasse, 1999).

Some methods such as mnemonic passwords, character substitutions or persuasive technology have been developed by the researchers to make memorizing complicated passwords easier for users (Singh and Singh, 2011). Check-off Password System (COPS) (Bekkering et al., 2003) is one of the distinctive examples which allows user to enter the characters of his password without regarding the sequence order. Therefore, user can use many alternative ways to memorize his password. Each user must select eight different characters in sixteen most commonly used letters. They are also allowed to use any letter more than once which might help to form stronger and more memorable passwords. It is claimed that COPS provides the advantage to form better passwords over the regular ones.

Semantic or *cognitive* passwords are created in the manner of asking questions to a user and treating the user's answers as a key to authenticate him. Renaud described an approach which relies on asking user some clarifying questions until he gives expected answers that match the system's ones (Renaud, 2003). Another provided technique expected user to answer a set of fact-based or opinion-based questions. These approaches are not user friendly as it most probably takes a long time for user to give the desired answer. Since users are willing to spare as short as possible time for authentication process, the cognitive based methods seem unlikely to be popular in computer systems.

One-time passwords are mostly used in some systems where protecting data is crucial such as bank accounts to provide higher security. It specifically provides a solution against the security vulnerabilities caused by user's behaviour like sharing passwords or writing down and leaving them somewhere accessible. It is also usable since the user is not expected to memorize complicated passwords. If hacker somehow obtains the password, he would not be able to reuse it after the first time.

6.2.3.2 Graphical Passwords

Graphical password authentication basically works like any other knowledge based authentication mechanism. The user is required to provide knowledge of a secret which he shared with the system beforehand. Contrary to the textual passwords, graphical authentication relies on visual memory. In both mechanisms, the user has to provide that secret in stored memory to the system (Renaud et.al, 2013). The fact that human's visual memory capabilities are far superior to their ability of remembering a string of characters.

This is because remembering information which is not part of a context is difficult for human brain. However, an image generally presents a context by itself (Bensinger, 1998). There are some studies that substantiated the ability of the human brain to recognize images easily. In the first study of Standing, Conazio and Haber, (1970) a group of participants were shown 2,560 photos for a few seconds. The users were then asked to examine a set of images consisting the previously seen ones and the new images. Participants could identify the images seen before with 90% successful recognition rate. Another study was performed with a similar principle (Standing, 1973). The participants were shown 10,000 images in two days and they performed a recognition rate of 60%.

From the users' point of view, creating memorable passwords is preferred so they can recall it later. Similarly, in a graphical password scheme, a user needs to choose memorable click locations in an image (Wiedenbeck et al., 2005b). There are two important points about remembering those locations: first one is the nature of the image itself and the second one is the sequence of the click locations. Studies indicated that people have some difficulties to recognize individual objects in a mixed-up image. Images which have semantically-meaningful contents are easier to memorize since remembering arbitrary things is difficult for the human brain (Norman, 1988). The long-term memory stores a meaningful interpretation of the image instead of the image itself. This means unnecessary visual details will be lost. Users are free to find their own way to encode the information in their brain so they can recall the information to find the correct locations on the image later. However, to create a strong memory, information should be processed in a deep and meaningful way; so, it can be stored in long-term memory.

In terms of remembering, graphical passwords have been considered as a possible alternative for traditional passwords. Numerous studies have been done and various graphical password schemes proposed so far.

The first graphical password scheme was proposed by Blonder in 1996 (Blonder, 1996). Within this scheme, pre-defined tap regions were used on an image to create a password. The user had to enter his password by clicking on these regions in a specific order. This scheme has significant security drawbacks as it is vulnerable to shoulder surfing attacks and has a pre-determined and very small password space. However, this scheme formed the basis for some of the best graphical password schemes designed later.

Commonly, graphical passwords are classified into three categories which are recognition-based, recall-based and cued recall-based. In the following sections, several graphical password authentication schemes using different techniques will be reviewed. For each scheme, its design implementation, advantages and disadvantages will be discussed. Where appropriate, relevant studies conducted about the schemes will also be discussed as a foundation to understand the bigger picture of graphical passwords as the nearest alternative to traditional alphanumeric passwords.

5.2.3.2.1 Recognition Based Graphical Passwords

In recognition-based systems, users have to memorise a set of chosen images during password creation and then recognise their pre-selected images from among many different ones in order to log into the system. This type of scheme relies on exceptional human memory to recognise previously seen images, even those seen quickly. Currently, proposed recognition-based systems use images such as faces, random art pictures, daily objects and icons. The most extensively studied graphical passwords are Passfaces (Passfaces, 2009) and Dejavu (Dhemija and Perrig, 2000) and Story (Davis, Monrose and Reiter, 2004). The following sub-sections will discuss each scheme in detail.

Passfaces:

The first example of a recognition-based scheme which uses human faces as a verification tool for authentication process is Passfaces. In this technique, users see a grid of nine faces and selects one face previously chosen by the user as shown in Figure 6.1.

It offers two-factor authentication to provide a higher level of security which can be easily integrated into existing systems in different working areas such as financial, government, healthcare and corporate networks (Passfaces, 2009). Passfaces was based on the fact which is proven by some research and experimental studies which reveals that viewing and recognising faces leaves an impact on one's memory recognition. Hadyn et al. (1992) explain that face recognition is a kind of different process from general object recognition in the human brain; since neurological measurements indicate that our brains have a special component, a unique function, to recognise faces specifically. In addition,

the human brain does not need any conscious effort to commit faces to memory and it recognises the faces not recalls.

In order to enrol in Passfaces, users are first presented a number of faces (could be three to five faces) to view. In the familiarisation process they are required to familiarise themselves with these presented faces. The process begins with examining each face and trying to find similarities between the shown face and people they may know. Then they are asked to go through a face recognition exercise which requires them to select one of the presented faces from a grid of nine faces. Once the user has successfully recognised the correct faces, they are allowed to log in.

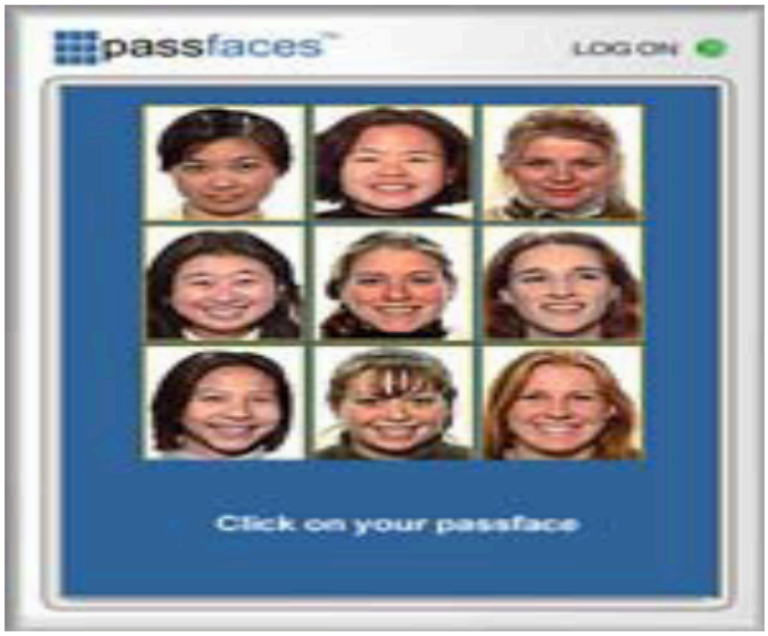


Figure 6. 1 Example of Passfaces

Davis et al. (2004) indicate that allowing people to choose the faces to create their password can lead to predictability issues since more attractive faces are most probably chosen frequently, thus significantly reducing the security. Dunphy et al. (2007) consider the social engineering attacks, by the way users are convinced by the attackers to describe the images in their portfolio. Their study results show that 8% participants could log in obtaining the portfolio images based on verbal descriptions. The results also indicate that if more or less similar decoy images to the portfolio images are used to reduce social

engineering attacks, it causes usability issues since recognising the correct portfolio images become difficult.

Later, Everitt et al. (2009) preferred to investigate the Passfaces scheme in terms of the effect of frequency access on a graphical password. They examined interference effect resulting from interleaving access to multiple graphical passwords and patterns of access while training. In a five-week period users were directed to log on to four different accounts according to different schedules. The results demonstrated that users who logged in more frequently were more successful at remembering their passwords. This study is the first of its kind in graphical password domains looking into the issues and effect of having multiple graphical passwords, as people commonly need more than four passwords. Thus, the effects of interference are even more crucial in a widespread deployment of graphical passwords. Unlike similar studies that examine only single graphical passwords, these findings discuss more realistic evaluations of multiple graphical passwords usage.

DejaVu:

DejaVu was proposed by Dhamija and Perrig (2000) to point the drawbacks of traditional alphanumeric passwords and PINs. In general, DejaVu consists of three major phases; portfolio creation, training and authentication. During the portfolio creation phase, users select a specific number of images from a larger set of images presented by the server. Figure 6.2 shows some images from the image selection phase in their proposed prototype system. Dhamija and Perrig suggest that the strategy of choosing images from random art instead of photographs reduces the predictability of the portfolio, hence increasing the security of the system. They believe that the images of random art are more difficult for users to write down as their password or to share with others by describing the images from the portfolio.

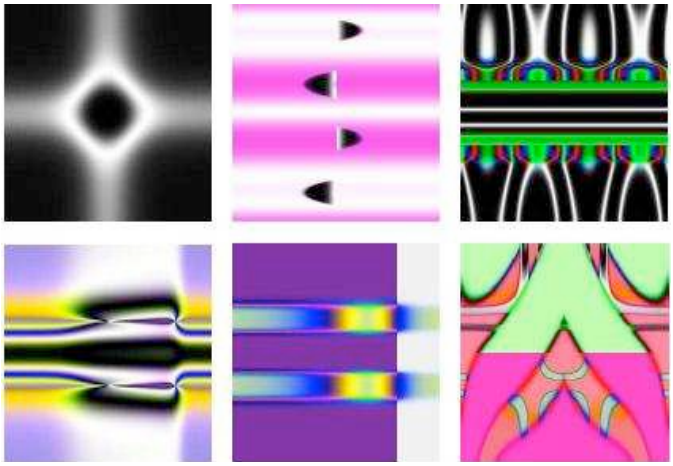


Figure 6. 2 Selection of random art images in DejaVu scheme (Dhajima and Perrig, 2000)

Next phase is a training phase, where users choose the images in the portfolio containing a set of decoy images. A secure environment must be provided during the selection and training phase to guarantee that no other person can see the image portfolio. Then in the authentication phase, a user will be validated if he manages to identify all portfolio images correctly among the decoys. In the prototype system, a panel of twenty-five images is displayed, five of which belong to the user's portfolio. The authors of this scheme propose that a fixed set of 10,000 images is adequate, but the attractive images should be hand-selected to increase the likelihood that images have similar probabilities of being selected by users.

Since it uses abstract images which help to decrease the risk of social engineering attacks which is trying to gather enough information to log in by tricking the user into verbalising their password, DejaVu scheme is advantageous. Similarly, it would seem difficult to identify images belonging to a particular user based on knowing other information about the user; however, problems resulting from predictable user choice remain possible, whereby users might make their choices based on favourite colours or shapes. Moreover, the usability issue was raised due to the fact that no feedback was given when users click on particular images, making it difficult for a user to be certain whether an image has been selected, which is obviously for security since providing too much feedback might lead to security being compromised.

Story:

Story is another recognition based graphical password scheme which is similar to

the Passfaces scheme. In the Story scheme, users create their passwords by selecting a sequence of k images from a single set of $n>k$ images to make a "*story*". Each image is drawn from a distinct category of image types which are capable of producing $n! / (n - k)!$ choices (Davis, Monrose and Reiter, 2004). The image category of the Story scheme is based on nine categories; animals, cars, women, food, children, men, objects, nature and sports. Example of images in Story scheme can be seen in Figure 6.3.

Figure 6. 3 Example of images in Story scheme (Davis, Monrose and Reiter, 2004)

6.2.3.2.2 Recall Based Graphical Passwords

These passwords are required for users to extract the information from their memory just as the traditional password authentication does. Since recall is a cognitively difficult task for users, they tend to adopt coping strategies. Different recall-based graphical password schemes will be presented above.

Draw-A-Secret:

The first example of recall based graphical password authentication mechanism is Draw-a-Secret (DAS) which was proposed in 1999 (Jermyn et.al, 1999). The approach expects a user to draw his authentication secret to be allowed to access an application. These should be more memorable than passwords because they take advantages of human's visual, lexical and kinaesthetic memory power (Renaud and De Angeli, 2009). DAS relies on the underlying grid sectors rather than drawings from a semantic perspective. According to Thorpe and Oorschott (2004), symmetrical graphical secrets

are the main concern as symmetrical drawings can be recalled more easily. They argue that an attacker could create a dictionary of possible symmetrical secrets and use it to compromise DAS which would take only six days to crack if the password is symmetrical. Then Nali and Thorpe (2004) conducted a user study with 16 participants to see if DAS secrets generated by users demonstrated any patterns. Some patterns are observed as the result of the study. While 45% participants created symmetrical drawings, 56% of them created centred ones. 80% of the drawings used less than three strokes. Considering these results as symptomatic of a larger user-base, the authors argue that DAS have a much smaller, practical password space. Figure 6.4 illustrates an example of DAS algorithm.

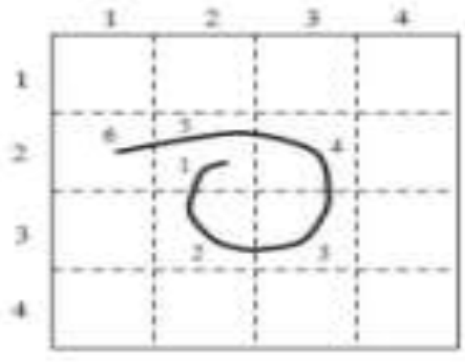


Figure 6. 4 An example of Draw-a-Secret (DAS) algorithm (Jermyn et.al, 1999)

Grid Selection:

Thorpe and van Oorschot (2004) proposed the Grid selection algorithm as a recall based graphical authentication scheme (see Figure 6.5). According to their design, users choose a small grid for drawing within a larger selection grid which increases the complexity of the password. After this, users zoom in their selected small piece of grid and create a drawing like in the Draw-a-Secret (DAS) scheme. This technique increases the password space however, it increases the users' memorability burden and input time of the password. It increases the security by sacrificing the password usability and memorability (Suo, Zhu, Owen, 2005; Sreelatha et al., 2011).

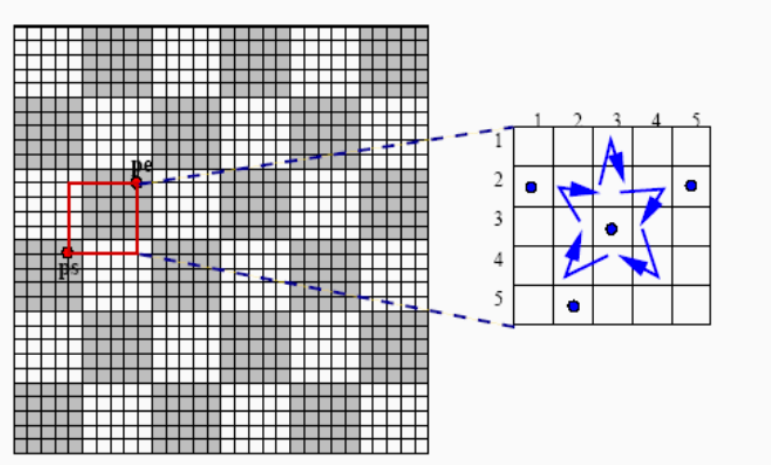


Figure 6. 5 An example of Grid Selection Algorithm (Thorpe and Oorschot, 2004)

GrIDsure:

An authentication scheme called grIDsure (see Figure 6.6) is another recall based approach that relies on knowledge of a secret pattern as well (Brostoff, Inglesant and Sasse, 2010). It presents a 5x5 grid to users and requires them to create a sequenced pattern on the grid. The users use the same grid during authentication, but the values between 0 and 9 in each of the 25 cells are changed since these values are randomly generated for each authentication attempt and are not unique to a cell. The user-generated secret pattern is applied to the grid to create the authentication secret. Bond (2008) identified some critical security deficiencies in this scheme and managed to identify the user's secret using only two fake authentication grids.

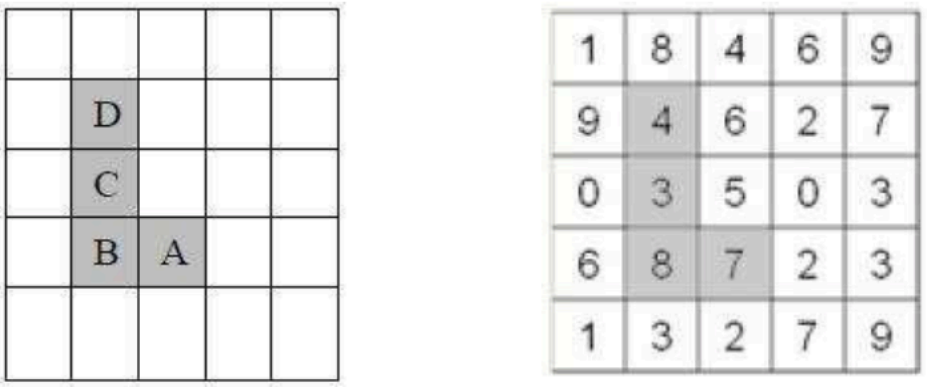


Figure 6. 6 An example of GrIDsure algorithm (Brostoff, Inglesant and Sasse, 2010)

Android Screen Unlock:

One of the recent draw-metric mechanisms is the common Android lock-screen pattern authentication. Such pattern based authentication mechanisms are also vulnerable to shoulder surfing attacks since observations of smudges on the device touch-screen are getting to become one of the common attacks (Aviv et.al, 2010).

5.2.3.2.3 Cued Recall Based Graphical Passwords

These passwords are created based on the information which is extracted from memory when users are given cues. The user can also create their password with their answers to a set of questions asked by the system like Zviran and Haga's associative passwords (1990). In their scheme users provide some information at the enrolment phase and later this information is used by them for reminding their passwords at authentication. In this category the most extensively studied graphical passwords are PassPoints and Cued Click Points which will be discussed in the following sub-sections.

Passpoints:

The PassPoints scheme was developed by Wiedenbeck et al. (2005b) based on Blonder's (1996) original idea that achieve solutions to defeat its limitations of needing simple, artificial images, predefined regions and consequently many clicks in a password (see Figure 6.7). PassPoints allows any image to be used. A user can click on points on an image to create a password. The image itself obviously acts as a cue to help the user remember their click-points.

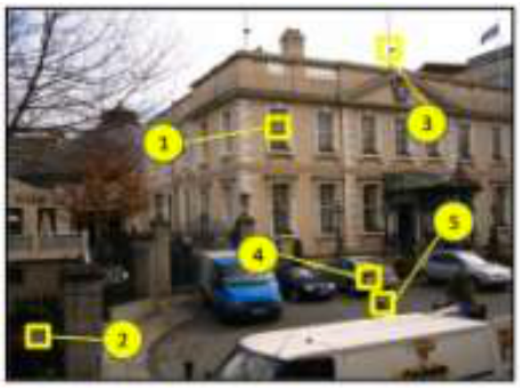


Figure 6. 7 An example of PassPoint algorithm

Security analysis on PassPoints revealed that the scheme is vulnerable to "hotspots" and its users tend to use similar simple geometric patterns with images. Hotspots are particular areas in an image which users select more commonly than others as part of their passwords. Hotspots are problematic since attackers can predict the hotspots in an image to consider the users' visual perceptions and their image choosing tendencies. Then they can build a dictionary of passwords containing combinations of these possible hotspots. This is the major drawback of PassPoints which is aimed to develop in an amended version called Cued Click Point scheme to overcome the hotspots problem.

Cued Click Points:

The technique of Cued Click points (CCP) reduces some of the drawbacks of the passpoints. In this method users have to click on one point per image on five different images shown in sequence (Chiasson, van Oorschot and Biddle, 2007). After each click another image is displayed. The displayed image is determined based on the previously selected click point. While logging on legitimate users have to click on the same click points in the sequence of image. If users select any wrong click points, authentication failure is indicated at the end of the login process (Chiasson et al, 2008; Mathew and Thomas, 2013). Figure 6.8 illustrates the implementation of CCP.

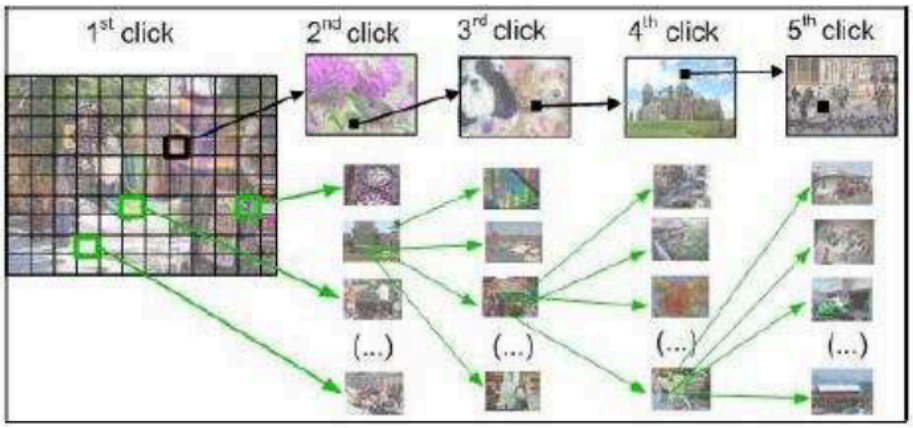


Figure 6. 8 Implementation of CCP (Chiasson, van Oorschot and Biddle, 2007)

Persuasive Cued Recall Points:

As mentioned in Chapter 3, persuasive technology is an approach to influence the people to behave in a desired manner. It is used to create stronger passwords by encouraging users to select random points in an image (Forget et al., 2008). Persuasive technology is used to reduces the drawbacks of text passwords and the hotspot problems of graphical passwords (Chiasson et al., 2008). Results of the studies tested the existing CCP schemes showed that hotspot problem remained with them. For this reason, a persuasive feature is added to CCP and it is then called persuasive cued click points PCCP to overcome the hotspot problem. PCCP (Chiasson et al., 2012) is used to encourage users to select less predictable passwords by using a randomly positioned viewport for users to click on (see Figure 6.9). Users can only select a click point within that viewport but they can use a shuffle button to randomly reposition the viewport in the registration phase. The shuffle button and viewport disappear and the images are displayed normally in the login phase. To login successfully, the users have to correctly click on the tolerance squares of the previously selected points on the image during login stage.

Figure 6. 9 Password Creation in PCCP (Chiasson et al., 2012)

PCCP increases the security, however, the susceptibility to surfing attacks remains

with PCCP. Also, it has some usability issues as it is difficult for the users to remember many images in the login phase. There have been many studies conducted recently to improve persuasive cued click points. Some of them integrated the scheme with text passwords (Ramesh, Venkateswarlu, Raju, 2015; Shrikala, Deshmukh and Pawar, 2013; Van Oorschot and Wan, 2009)

6.3 SUMMARY

Text passwords are the predominant authentication mechanisms in the information security field for years. As they have known security and usability issues many alternatives have been proposed so far.

Alternative solutions to the password problem such as biometrics, security tokens and smart cards resolve the memorability problem of text passwords. However, these authentication methods have some issues with privacy, theft, and the huge infrastructural costs of deployment and maintenance (Herley and van Oorschot, 2012).

On the other hand, knowledge-based authentication (KBA) has several advantages, being relatively easy to implement, not requiring additional hardware, inexpensive implementation and modification, and they are theoretically very secure. However, experience and research especially with text passwords has shown that they can be difficult for users to remember, which results in a loss of usability and security (Forget, 2012). Graphical passwords have also several drawbacks such as susceptibility to shoulder surfing and guessing attacks. They are not widely deployed as most users adhere to traditional passwords and do not prefer to change their authentication method.

There have been many different proposed solutions to solve the problems of existing text and graphical passwords, including biometrics, novel authentication schemes, password managers, single sign-on and one time passwords (OTP).

None of these approaches have yet been widely adopted by users. Therefore, users continue to adopt several coping mechanisms to deal with the memorability problems of text passwords. Towards solving this password problem, an authentication scheme should support users in creating secure, memorable, and usable passwords.

This chapter reviewed the most common alternative password authentication methods mentioning both their advantages and drawbacks. The next chapter introduces a novel hybrid password authentication scheme integrating text and graphical passwords.

CHAPTER 7

A NOVEL HYBRID PASSWORD AUTHENTICATION SCHEME BASED ON TEXT AND IMAGE

7.1 INTRODUCTION

User authentication is one of the most important parts of the security of information systems. The most common approach for authenticating human users is text passwords. Users generally choose weak passwords to remember them easily (Adams and Sasse, 1999; Yan et al, 2005). This increases the possibility of the passwords to be hacked by attackers. When users are requested to create long and complex passwords, they resort to coping strategies such as writing passwords down or reusing them (Burnett and Kleiman, 2006). Therefore, text-based passwords suffer from various drawbacks such as vulnerabilities to dictionary attacks, brute force attacks and social engineering.

Graphical passwords are considered as a good replacement for textual passwords. The fact that humans can recognize and remember images easily over text can be a solution to the memorability problem (Shepard, 1967). However, they are more vulnerable to shoulder surfing attacks as compared to textual passwords. Also, the graphical password authentication is relatively expensive to implement which prevents it becoming widespread.

To overcome the weaknesses of text and graphical passwords, this chapter proposes a hybrid authentication scheme which is a combined approach of text and graphical passwords.

The proposed scheme has many advantages in terms of security and usability. It allows users to create and memorize cryptographically strong passwords easily. It eliminates the risk of passwords being hacked by dictionary attacks. It also secures the passwords against shoulder surfing attacks. It is a user-friendly authentication scheme.

A hybrid authentication method is proposed to strengthen text passwords by using the images as an assistant tool for users to memorize complex character sets. Theoretically it is a text password scheme integrating user chosen and system generated characters. However, users are allowed to choose images from image portfolios to enter the system

generated characters associated with the images. In this approach, users continue to use text passwords, but strong and memorable ones. They do not have to remember complex passwords at first or write them down; with the help of the images they will be able to memorize them naturally.

Many hybrid authentication schemes have been proposed in recent years to overcome the drawbacks of knowledge based authentication schemes. While some researchers integrated different types of graphical passwords (Haque and Imam, 2014), others combined graphical passwords with text passwords (Mokal and Devikar, 2014, Rao and Yalamanchili, 2012; Sreelatha et al., 2011; Zhao and Li, 2007; Zheng et.al, 2010). These researchers proposed solutions to shoulder surfing attacks to strengthen the graphical password schemes. Rao and Yalamanchili (2012) proposed two authentication schemes using graphical passwords called Pair Pass Char (PPC) and Tricolor Pair Pass Char (TPPC). These both schemes support two modes of input: keyboard entry and mouse clicks. The first mode is the text mode and the other one is the graphical mode. The researchers carried out an experiment with 20 graduate students and found that the average login times increase as the password length increases in both schemes. The study also showed that the login times for TPPC scheme is higher, and rules for this scheme are more difficult to be applied. PPC scheme provides passwords as much as that offered by conventional password systems and it is greatly enhanced in the TPPC scheme as it uses the same character set in three colours. This proves that the login times increase much where the password space is enhanced in these proposed schemes. This means that these proposed schemes sacrifice the usability for security.

Zhao and Li (2007) proposed S3PAS which is a scalable shoulder-surfing resistant password authentication scheme. S3PAS is designed to be used in client/server environments. It integrates both graphical and textual password schemes and aims to provide resistant to shoulder surfing, hidden camera and spyware attacks. In this scheme two kinds of password are generated: original passwords and session passwords. Users create original passwords when they create their accounts and input different session passwords in every login process to protect their original passwords from releasing. There are some drawbacks in this system similar to other text based graphical password schemes. S3PAS schemes include complicated and longer login processes. Thus, the researchers plan to design a simplified version of S3PAS with a little lower security level

to increase its adoption in the future (Zhao and Li, 2007).

In another study, two authentication techniques based on text and colours are proposed (Sreelatha et al., 2011). These techniques are called pair-based authentication scheme and hybrid textual authentication scheme which are suitable for Personal Digital Assistants (PDAs). Both the techniques use grid for session passwords generation. The researchers claim that these schemes are resistant to shoulder-surfing, dictionary and brute force attacks. However, they did not conduct a detailed user study to evaluate the security of the schemes. They only measured the registration and login times of the passwords created with these schemes by 10 participants. Since these schemes are completely new to the users and there is not a proper security and usability analysis of them, these proposed techniques should be verified extensively for security usability and effectiveness in the future. Similarly, there is not any user study conducted to test the security and usability of another text-based shoulder surfing resistant graphical scheme proposed by Chen et al. (2013).

Zheng et al. (2010) also proposed a hybrid password scheme based on shape and text. The proposed scheme uses shapes of strokes as origin passwords and allows users to login with text passwords via traditional input devices. Although the researchers claim that the scheme is resistant to shoulder surfing, hidden camera and brute force attacks and that it has variants to strengthens the security level through changing login interface of the system, the scheme still has some security and usability drawbacks. It is not familiar to users so they may adopt simple and weak strokes. This increases the chance of attackers to obtain the passwords. Also, the password creating step is vulnerable to attacks since users have to tell the system the original shapes and strokes. Moreover, the login process of this scheme is longer than other graphical schemes. For these reasons, more advanced authentication system should be proposed to improve this method.

In a recent study, a comprehensive survey on shoulder surfing resistant text based graphical password schemes is conducted (Mokal and Devikar, 2014). This study explained the existing security problems, possible solutions and limitations of some of these schemes.

These studies primarily focused on the existing shoulder surfing attacks in text based graphical password approach. However, a guessing attack is also a potential

problem for graphical password schemes because of the predictability of user-chosen graphical passwords (Van Oorschot and Thorpe, 2012; Vorster and Van Heerden, 2015a).

All the aforementioned schemes have discrete text and graphical password creation steps which considerably increase the registration and login times. Compared to these schemes, the novel hybrid authentication scheme introduced in this research shortens password creation and login times as it has an integrated registration phase. Unlike other schemes, in the proposed scheme, images are used as cues to help users to complete their complex text passwords instead of creating a second password. Thus, the proposed scheme improves recall rate without sacrificing the security against attackers. Moreover, the results of the previous studies showed that users have an adoptability problem with these schemes as they are unfamiliar to users. However, the proposed scheme substantially preserves the login experiences of users who are accustomed to traditional textual passwords. As far as is known, the proposed scheme is the first scheme in the literature associating the letters of the chosen text passwords with the images by using the Tip of the Tongue (TOT) phenomenon. This feature significantly increases the memorability of the passwords.

The next sections describe the proposed scheme in detail considering its security and usability aspects. Also results and analysis of an empirical study which is conducted to evaluate the effectiveness of the scheme are presented in the following sections.

7.2 THE PROPOSED AUTHENTICATION SCHEME

Considering the popularity and wide deployment of text passwords, they seem to be used as a prevalent authentication mechanism for many years to come. Thus, this chapter suggests that effort should be made to enhance text passwords by increasing their password space and memorability with an additional mechanism based on images. The combination of text and images are likely to increase resistance to some password attacks, such as brute force and observing attacks. To this end, a hybrid authentication scheme integrating text and recognition-based graphical passwords is proposed in this chapter. This authentication scheme can also reduce the phishing attacks because if users are deceived to share their key passwords, there is still a chance to save the complete password as attackers do not know the users' image preferences.

Beside the security aspect, the proposed authentication scheme aims to increase memorability as it gives chance to users not to be have to remember long and complex passwords. Thus, with the proposed scheme users will be able to create strong passwords without sacrificing usability. The hybrid scheme also offers an enjoyable sign in / log in experience to users. The details of the design and security-usability analysis of the scheme are presented in the following sections.

7.2.1 Design of the Proposed Scheme

To test the proposed authentication scheme, a web application which also works on mobile phones is designed and implemented. This web application uses ASP as the server side programming and JavaScript as the client side programming. MS SQL database is used to store the data.

The design process of the proposed authentication scheme is as follows:

- ***Identify the Problem:*** Improving the security and usability in the knowledge-based authentication schemes. The challenge, limits and possible solution.
- ***Explore:*** Reviewing the previous related works. Examining the security and usability problems in the existing text and graphical based authentication schemes.
- ***Design:*** Designing a hybrid authentication scheme ensuring security and usability at the same time.
- ***Implement:*** Implementing the designed scheme.
- ***Test and Analyse:*** Conducting empirical studies to test, analyse and evaluate the security and usability of the scheme.
- ***Improve:*** Improving the design according to results of the empirical studies.

The proposed scheme is designed using Persuasion Technologies (PT). PT functions as a tool and social actors to communicate with users and increase their capability to perform a target by making it easier for them (Fogg, 2002). Accordingly, a help feature which visualize the password creation instructions for users is designed in this scheme to help users to create passwords easily (see Figure 7.3).

User authentication process in the designed scheme has two main steps: registration phase and login phase. The registration phase consists of creating key passwords and image selection. The reasons behind key design decisions and how they relate to security and usability considerations are explained at every stage of the registration and login phases in the following sections. The flowcharts of the registration and login phases of the proposed authentication is illustrated in Figure 7.1.

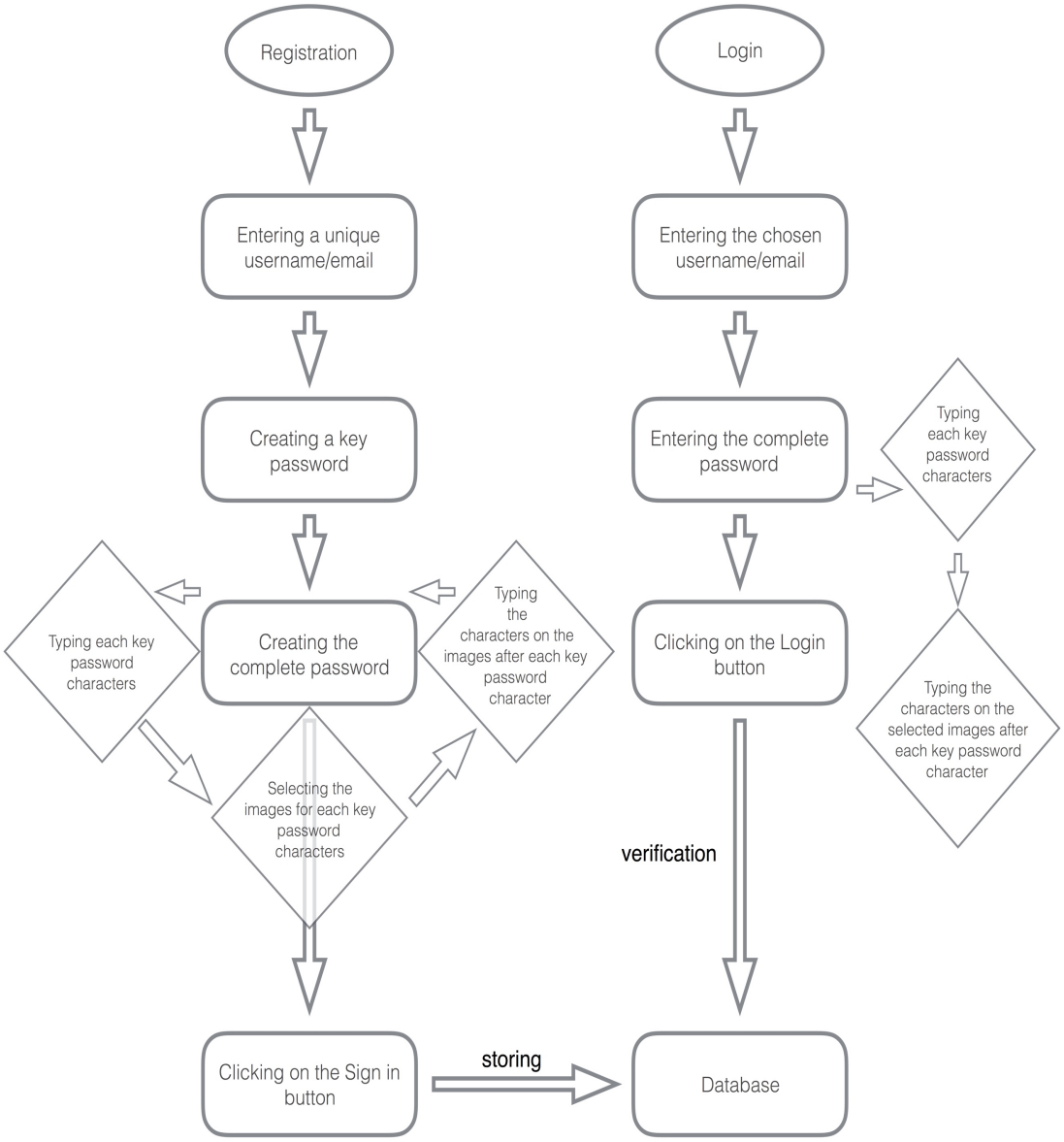


Figure 7. 1 The flowchart of registration and login phases

7.2.1.1 Registration Phase

. In the first step of the registration phase, users are asked to enter their username or email address in the username field.

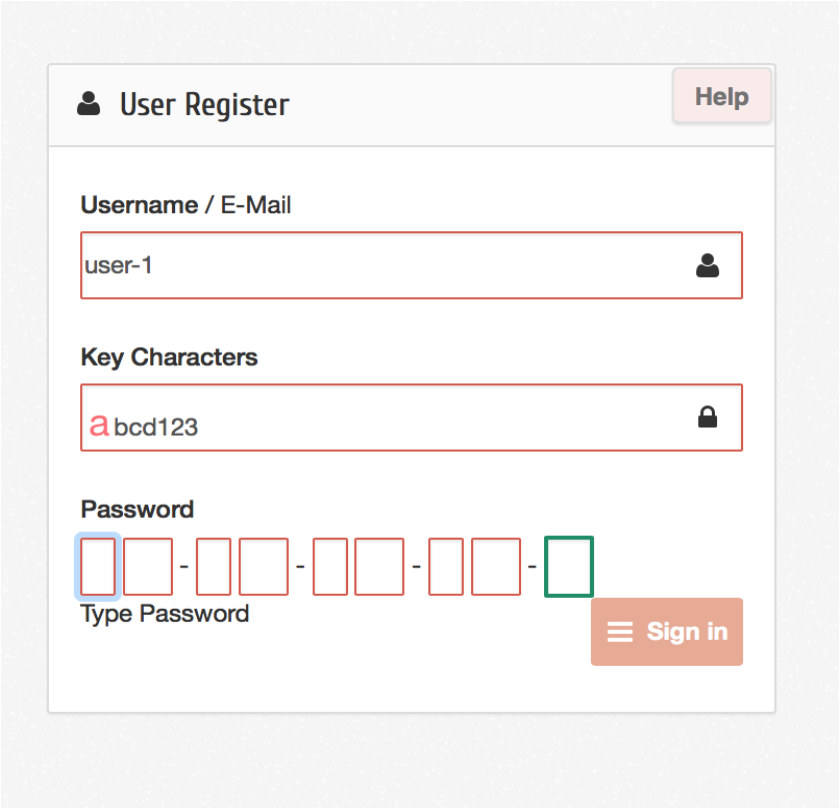
. Then they are asked to create a key text password called key characters. The only restriction about the key password is that its first 4 characters should be alphabetical which can be either upper or lower cases allowing for users' preferences. The reason why the minimum length of key password is set to four characters is that every user can remember it easily. The theoretical password space calculated in this way have satisfying results to provide high security.

. After creating the key password, the image selection process begins. This is an integrated process of retyping the key password and choosing the images. While users retype their key passwords in the "password" field, an associated image portfolio appears each time they type a particular letter. For each typed letter, there is a related image portfolio consisting of 20 images. This relation comes from the idea of choosing images of objects, famous people, activities or known figures which their names' initials is the typed letter. It means, for example, when users type "a", as a character in their key passwords, an image portfolio appears including images whose names' are starting with "a" (the images of alpha, apple, Albert Einstein etc.). Then users select the images from the appeared image portfolio at their own choices. Users have to select an image from each sets of images. This selection will be performed so as users type the characters under the images into the password field but not click on the image. There are a set of two random characters under each image combining one alphanumerical character and one digit or letter. Briefly, users will enter these two-characters after each character of their key password. To make it easy for users to recognize which characters they should enter, the password field is designed to include small and large squares. The small squares coloured in green is to enter each character of key passwords, and the larger squares coloured in red is to enter the characters under the images. This helps users not to be confused of the order of the characters. In this study, users are expected to choose four images in total which are associated to four letters in their key password, considering the memorability issues. Therefore, there are four small green squares for the first four alphabetical

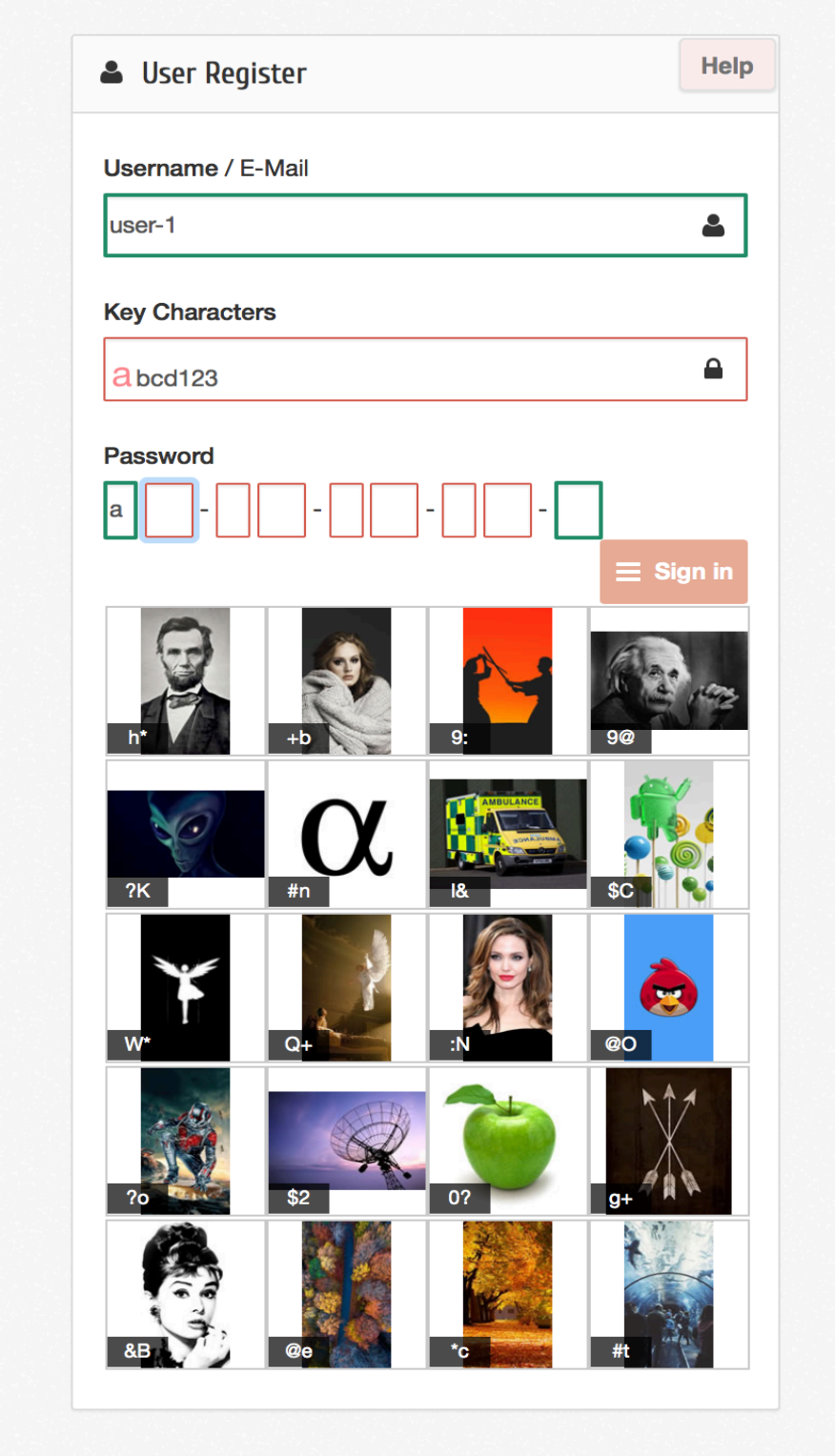
characters of the key password. Also, there are four larger red squares for the two sets of characters placed under the images. The last large square is to enter the rest of the key password's characters.

The number of images in each portfolio is set for the first test of the scheme. The theoretical password space calculated in this way have satisfying results to provide high security.

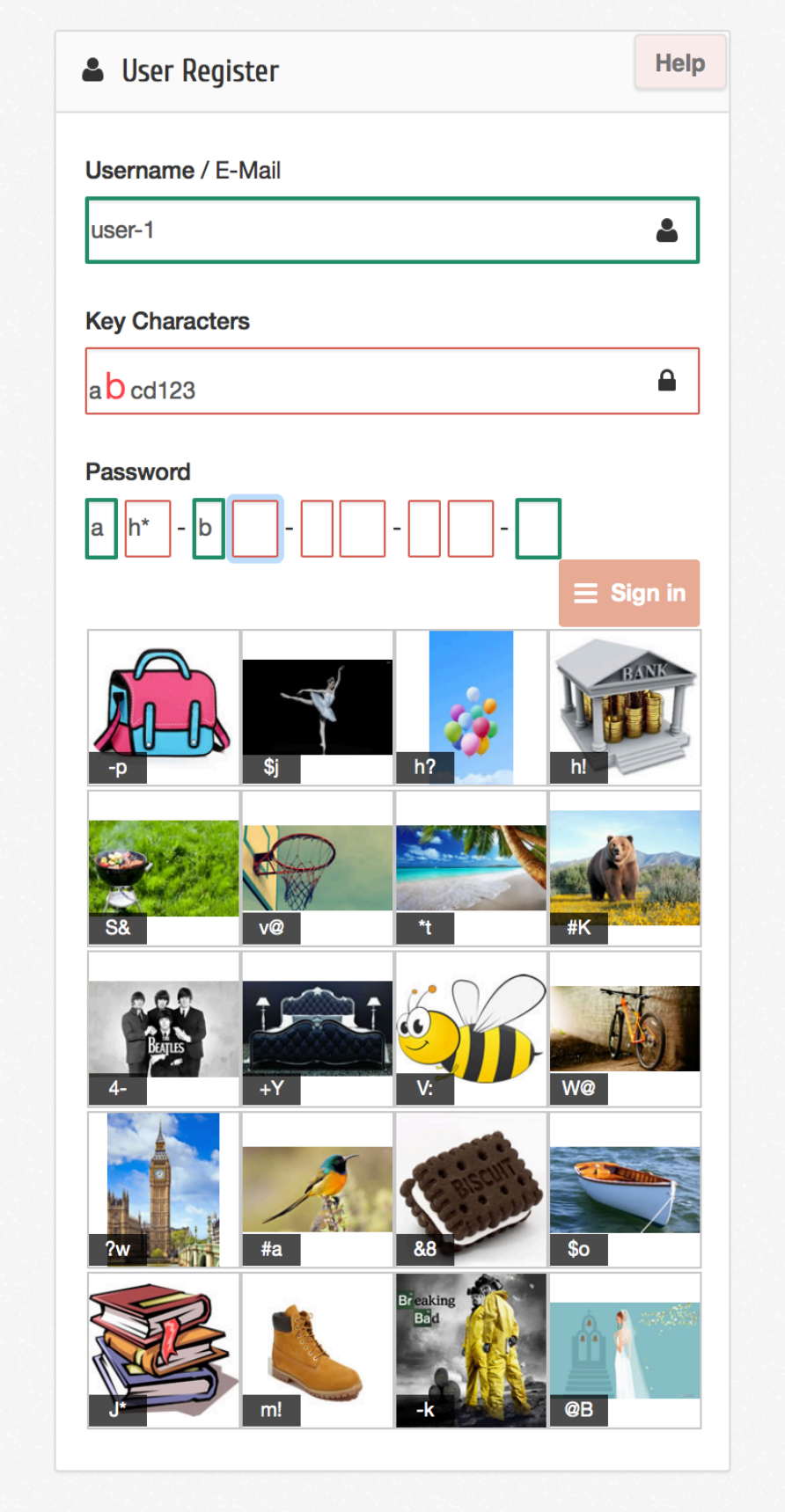
This progress allows users to create a complex password mixing their key passwords and the random characters associated with the selected images. The characters under each image change for different users. The registration phase of the scheme is illustrated in the Figure 7.2 (a-e) step by step with the example username, *user-1*, and the password, *abcd123*.



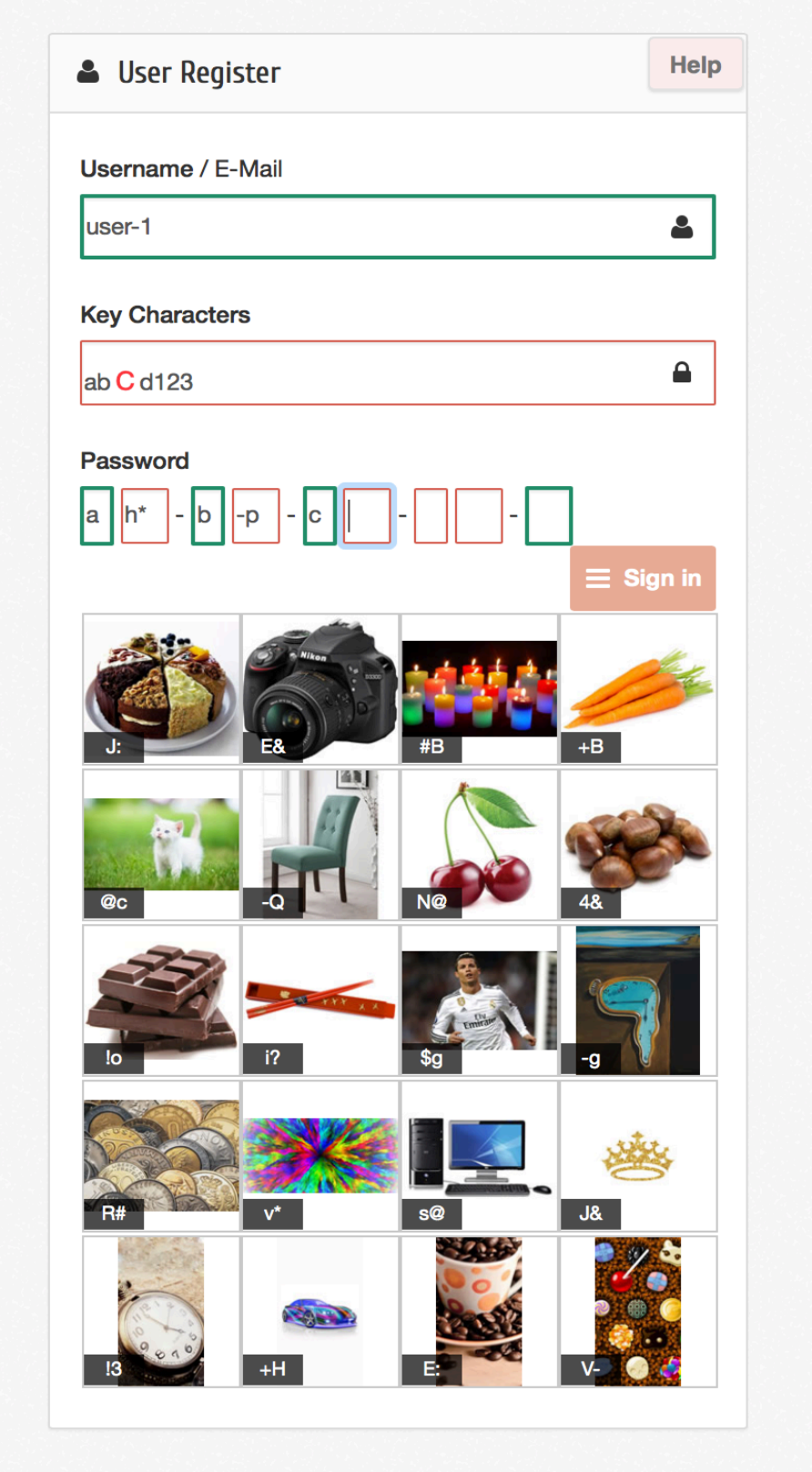
a-Entering the username and the key password (key characters)



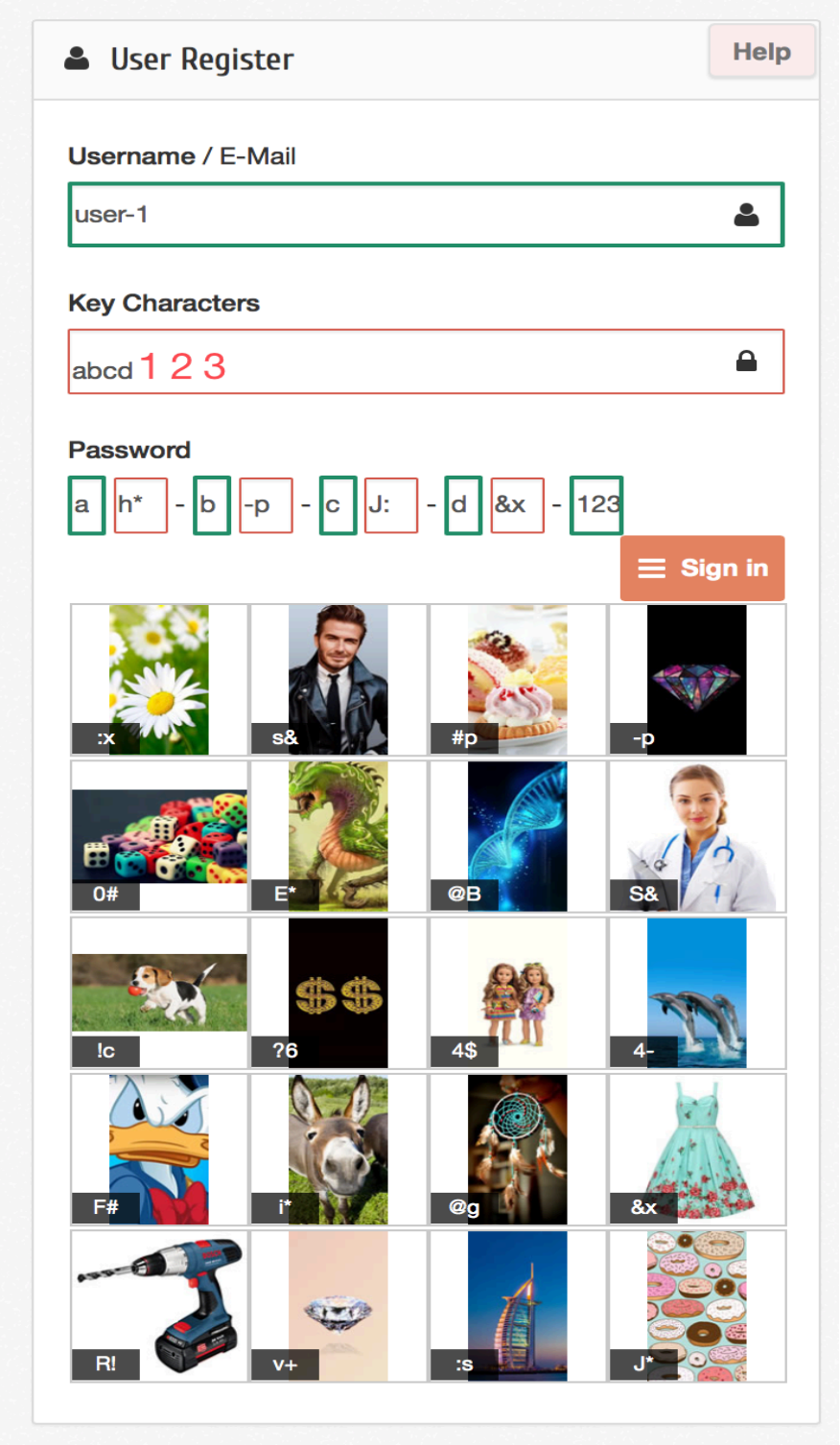
b- Entering the first character of the key password and characters under the selected image from the portfolio



c- Entering the second character of the key password and characters under the selected image from the portfolio



d- Entering the third character of the key password and characters under the selected image from the portfolio



e- Entering the fourth character of the key password, characters under the selected image from the portfolio and rest of the characters of the key password

Figure 7. 2 (a-e) User registration phase of the proposed scheme

As seen in the figures, the password “abcd123” which is created as the key password by the user whose username is “user-1” turned into a complex password “ah*b-pcJ:d&x123” including upper case, lower case, number and special keyboard characters at the end of the experiment. The user chose the images of Abraham Lincoln, bag, cake and yellow dress and entered the characters under those images. The user does not have to remember the complex, 15 characters long password as remembering the key password and those four images will be enough to login successfully. Even if users create four characters long password composed of only lower cases, it will turn into a complex, unpredictable password including different type of characters when the password creation process ends.

The proposed scheme has a help feature which visualize the password creation instructions for users step by step (see Figure 7.3). When users click on the “help” button on registration phase, they will see a slide of instructions to create a password with the scheme, which they can pause at any stage.

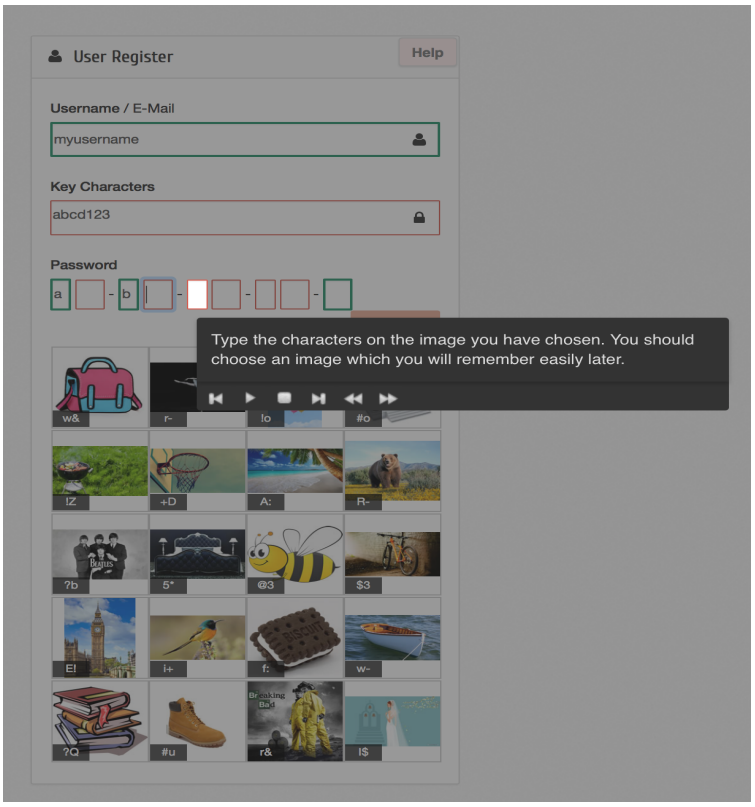


Figure 7. 3 Slide of password creation instructions for users

. When creating the mixed password is finished, the sign up button will be active, and users are allowed to click it to complete their registration. All the details including

username and complete passwords entered in the registration phase are stored into the database which will be used during the login phase for the verification.

7.2.1.2 Login Phase

. In the login phase users are asked to enter their user name/email and their passwords (mixed password). Users will be able to see the images like in the registration phase but the order of images within the set will be random at every login time. After a while as users continue to login the system, they will be able to memorize their complex passwords so they might not need to look at the images. The system has a feature which allows users to hide pictures whenever they want. This decreases the susceptibility shoulder surfing attacks. In case they have difficulties to recall the part of their passwords, they can view the images by simply ticking the "invisible pictures" box. The screenshot of the login phase of the authentication scheme is shown in Figure 7.4.

.

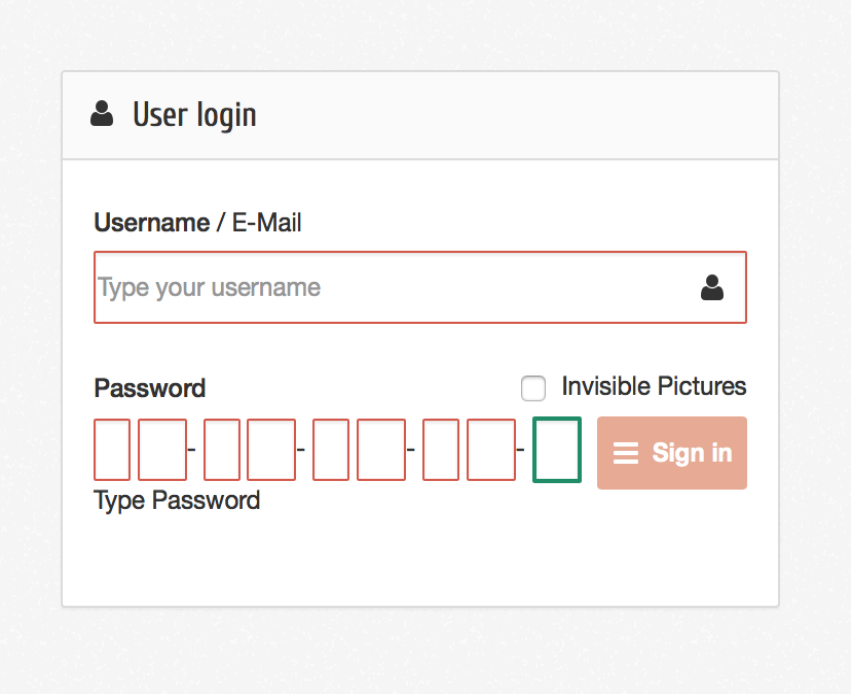


Figure 7. 4 User login phase of the proposed scheme

In the login phase, while supplying the username/email and password information,

independent of whether or not they match those defined during password creation, the image portfolios will continue to appear based on the typed character. Users must correctly enter the characters under all images pre-chosen for their accounts in each round of password verification. If any information is wrong, the user will be shown a “access denied” message at the end of the login phase. Seeing an image portfolio including no familiar image allows legitimate users to immediately realize that they entered a different character from key password’s characters and gives them chance to fix it. However, this prevents an attacker from knowing that the characters tried are invalid.

. After the successful entries of both username/email and password, the users are allowed to access their accounts.

This section presented the details of the design of the proposed hybrid authentication scheme. The security and usability aspects of the scheme is discussed in the next section.

7.2.2 The Security and Usability Analysis of the Scheme

The following sections presents the security and usability analysis of the proposed scheme. Password space of the scheme is formulated and its resistance to attacks is discussed under the security analysis. Password creation and login time and memorability of the passwords created with the scheme is discussed under the usability analysis.

7.2.2.1 Security Analysis

A new password scheme should allow users to create passwords which are strong enough against guessing, brute-force and observation attacks. The quality of a password authentication scheme depends on how it is effective to limit attempts to guess users’ passwords either by people who know them or a computer-based cracking program trying the possible passwords (Haque, Imam and Ahmad, 2012; Haque and Imam, 2014). Password strength is determined by measuring the password space which is the maximum possible number of passwords generated by the system. The password space of the novel authentication scheme is formulated in the following section.

Password Space:

The strength of the proposed scheme can be evaluated by measuring both the entropy of the user chosen key-text password and the graphical password parts. Assume that the password space of the key password created by the users in our scheme is $P_{1,}$ the length of the key password is "l" and "n" is the numbers of the characters in an alphabet from which the key password's characters are randomly selected such as an alphabet including English upper and lower letters, digits and non-alphanumeric characters. The key password which is l characters long has an entropy of "l. $\log_2$ n" bits. In our scheme, however, this should be somewhat lower than this since at least four letters of the key password must be either upper or lower case so we calculate the password space of the key password in two parts.

The password space for the key password is: P_1= (l-4). $\log_2 n_1$ x 4. $\log_2 n_2$.

To find the total password space, we also calculate the entropy of image based passwords. Let P_2 be the password space of image based passwords, and c be the number of rounds of choosing images from the related portfolios which is 4 in our case since at least 4 different images should be chosen from different portfolios. Assume that n is the numbers of images in each portfolio, and k is the number of images selected from each portfolio. The entropy of a randomly selected images and accordingly the two-character sets is: $P_2 = c \cdot \log_2 \frac{n!}{(n-k)!}$

The password space of the proposed scheme is: $P = P_1 \times P_2$

Choosing different parameters, for example increasing the values of k, n or c can increase security, but also decreases usability. We believe that remembering a key password and four images from different portfolios consisting of twenty images will not be a burden for users' memory, but it can increase the resistance to dictionary attacks by increasing password space in practice.

Text passwords used in practice are generally far from randomly and independently selected. Most of the user passwords consist of only lowercase or digits which significantly decreases the entropy. For example, a randomly generated 8-character password which is consisting of digits (0-9), lowercase (a-z), and uppercase (A-Z) has $8.\log_2 62 = 47.6$ bits of entropy if all characters were selected randomly and

independently. However, in practice they have far less bits than this (Van Oorschot and Wan, 2009). Considering the realistic scenario, the added security from image selection parts of the proposed scheme becomes more significant. The integrated scheme significantly decreases the possibility of successful dictionary attacks.

Resistance to Attacks:

As stated above, the proposed authentication scheme decreases the chance of attackers to obtain passwords via brute-force and dictionary attacks. The scheme has an integrated step of creating complex passwords based on text and images, which increases the numbers of possible passwords generated by the system, the password space.

While selecting the images and entering the associated characters, the input is given through keyboard rather than clicking on the images to prevent other people to observe the password over the user's shoulder. Allowing users to use mouse to enter the input maybe would make the system more adaptable but also more susceptible to shoulder surfing attacks. It supports client-server environment and its main advantage is it's resistant to brute force and shoulder surfing attacks. However, the handicap of the scheme is that people who look over the user's shoulder can find out the previous character of the key password when they see the image portfolio. They of course, will not know the preferred image as users do not click on the images but this is still a risk for part of the password. This might be prevented by not placing images of objects, foods or famous people whose names' initials is same in a portfolio, but we prefer to evaluate its efficiency on memorizing images.

7.2.2.2 Usability Analysis

The idea of associating the images with the letters in the key passwords to increase the memorability of the final complex passwords come from the phenomenon called *Tip of the Tongue (TOT).* The phenomenon refers to failing to retrieve a word from memory or partial recall but feeling that the retrieval is imminent (Brown, 1991; Encyclopedia.com 2004). It reveals that lexical access occurs in several stages. People who experience this phenomenon can often recall some features of the target word mostly *the first letter*, or its syllabic stress and words similar in sound or meaning (Brown and

McNeill, 1966; Schwartz and Metcalfe, 2011). The first letters of words are also important for coding words. For this purpose, phonetic alphabets are produced including code words which are assigned to each letter (Crystal, 2011). Users can code the words by assigning them to the letters in their key password to recall later. Associating the typed letters with images will help users to recall both the images and key characters.

Furthermore, to increase the memorability, the images in each portfolio are chosen from different categories including famous people, objects, sport activities, known art figures, animals, foods and places to be used in the authentication scheme similar to the Story scheme (Davis, Monrose and Reiter, 2004). This allows users to have many options in which they can select the most appropriate one to themselves as well as the most probable one remember.

This section discussed the security and usability aspects of the proposed scheme in general. To evaluate the effectiveness of the scheme an empirical study was conducted with users. The next section presents the details of the empirical study.

7.3 THE EMPIRICAL STUDY: EVALUATION OF THE SECURITY AND USABILITY OF THE PROPOSED AUTHENTICATION SCHEME

7.3.1 Introduction

An empirical study was conducted with the students studying in University of Sussex in order to evaluate the security and usability of the proposed hybrid authentication scheme. Beside the security and usability aspects, the study is also used to evaluate the user satisfaction of the proposed scheme.

To perform this study, an ethical approval was sought and obtained from the University of Sussex Sciences and Technology Cross Schools Research Ethics Committee (C-REC). The certificate of the ethical approval can be viewed in Appendix C.

The following sections presents the details of the empirical study.

7.3.2 Methodology of the Empirical Study

7.3.2.1 The Design and Apparatus

A web application was developed to test the security, usability and user satisfaction of the designed authentication scheme. The application also works on mobile phones enabling users to create strong passwords. The researcher's portable computer was used to collect data from participants during the empirical study. The apparatus used in this study are as below:

- A password register/login page of the designed authentication scheme
- A questionnaire for the participants
- Consent forms to read and accept for the participants

All the apparatus is included in the section Appendix C.

First, the participants were asked to create an account using the scheme and login afterwards. The participants were shown a register / login page to enter their username and create a password. The interfaces of the register / login page are as illustrated in Appendix C. Once the participants had registered the application, they were given the questionnaire to fill out. The questionnaire included 6 questions related to users' experiences and satisfaction with the scheme. Several studies that used similar materials to test the effectiveness of their schemes have been reviewed in the section 7.1.

The average time to complete the study including registration and filling the questionnaire was approximately 10-15 minutes.

7.3.2.2 The Procedure

At the beginning of the empirical study, the participants were assigned a unique ID number. This id numbers were used to match the participants' credentials and questionnaire responses. The participants were given a brief information about the study and asked to read and accept the consent form to participate. Once they had accepted the consent form, they were able to register the application. For those participants who were interested in getting more information about the study researcher's contact information

were provided in the consent form. After the participants registered the application successfully, they were asked to fill the questionnaire.

Participants were treated to chocolate and soft drinks during the study. At the end of the study, the participants were asked to login the websites after a week and a month to find out whether they recall their passwords.

Finally, participants were thanked for their participation in the study.

7.3.2.3 The Measurements

There are several measurements involved in the empirical study: password strength, password cracking time, password creation and login time, memorability and user satisfaction.

To measure the security of the new authentication scheme, created passwords were analysed using the "*Password Meter*" (Password Meter, n.d.) and "*How Secure is my Password?*" (Collider, 2016) tools same as the passwords created in the password guideline-advice study (see chapter 5). While the "*Password Meter"* measured the strength of the passwords created with the scheme, "*How Secure is my Password?*" measured the password cracking times.

The other elements measured in this empirical study were the password creation and login times. The researcher measured these while participants were testing the authentication scheme.

To measure the memorability, participants were contacted approximately after a week and a month, and asked to login the system again to understand whether they remember or not their passwords.

User satisfaction were measured based on questionnaire responses of the participants to evaluate the authentication scheme.

Next section presents the demographics of the participants in the study.

7.3.2.4 Demographics

52 students studying in the University of Sussex were recruited to participate in this empirical study. There were 29 females and 23 male participants. Undergraduate students as well as the postgraduate students participated in the study. While 33 of the participants were undergraduate students, 19 of them were postgraduate students. Figure 7.5 and 7.6 illustrate the demographic details of the participants involved in the empirical study.

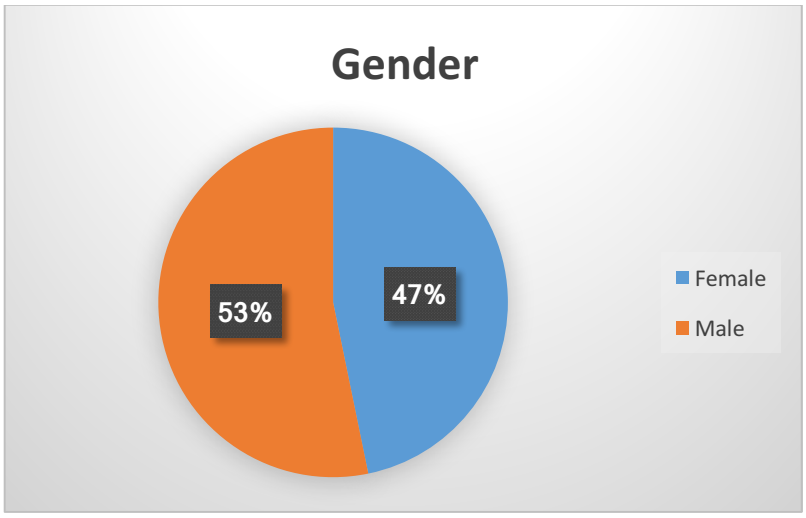


Figure 7.5 Gender percentages of the participants

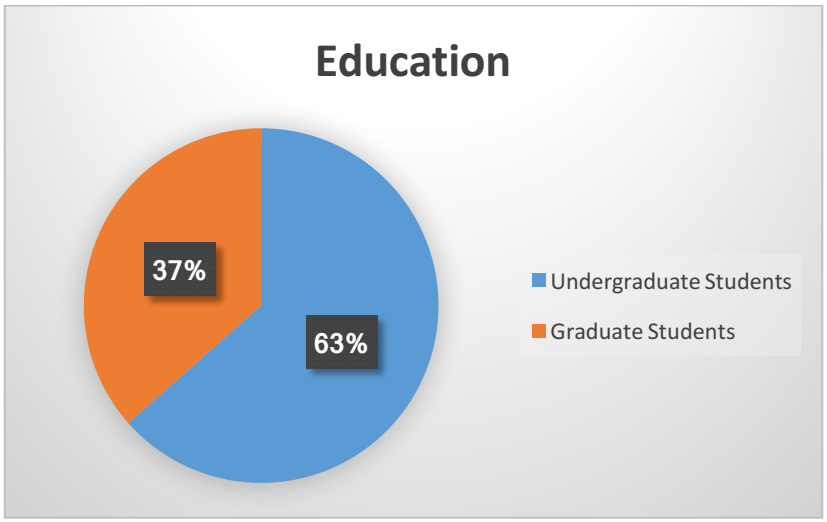


Figure 7.6 Education background of the participants

Usability and security evaluation of the scheme based on the analysis of the collected data is presented in the following sections.

7.3.3 The Results and Analysis of the Empirical Study

In the following sections, results and analysis of the empirical study are presented in detail.

7.3.3.1 The Password Analysis

Password Strength:

To evaluate the strength of the passwords created with the proposed authentication scheme, an empirical study was conducted with 52 participants. All the passwords created with the scheme were between 12 to 16 characters in length. Since eight characters come from the selected images provided by the scheme inherently, the length of user-chosen key passwords were 6 characters long on average.

The "*Password Meter"* is used as a tool to measure the password strength. All participants created passwords with this scheme, and all of them were strong passwords according to the measurement results. The passwords created by the participants were scored out of 100 and the least score was 81, whereas the mean password strength was M= 96.50 (SD = 5.96). However, this tool alone is not sufficient to determine the resistance of a password to cracking. The user-generated passwords should be strong enough to password guessing attacks. The next section discusses the password cracking times of the passwords created with the proposed scheme by the participants.

Password Cracking Time:

To find out the estimated cracking time of the passwords created with this scheme, the tool called "*How Secure is My Password*" is used like it is used for the password guideline-advice study in chapter 5. In line with the password strength, all passwords

were hard to crack, according to the measurement. Password cracking times were above decades and 41 out of 52 passwords would take more than a hundred years to crack.

Password Creation and Login Time:

The password creation time and login time of the participants were measured by the researcher during the experiment. Table 7.1 summarizes the time it takes to create a password and to login in seconds. It took about one or two minutes on average to create a password or to log in for participants.

Table 7.1 Password creation and login times in the empirical study

	Password Creation Time	Login Time
Proposed Authentication Scheme	M = 94.08 (SD = 19.93)	M = 57.40 (SD = 15.73)

Memorability:

Passwords created with the proposed authentication scheme were remembered correctly most of the time. Although there was a slight decrease from a week's duration to a month, still 75% of 52 participants remembered their passwords correctly, and successfully logged in to the system. Table 7.2 shows the login success rates after a week and a month period.

Table 7.2 Login success rates in the empirical study

	Login Success Rates (after a week)	Login Success Rates (after a month)
Proposed Authentication Scheme	90.38 % (47/52)	75.00 % (39/52)

The memorability of the passwords created in this empirical study was compared to those in the password guideline study presented in chapter 5. There is a trend of decline as time goes by, such that memorability after a week declines across all groups when

participants tried to remember their passwords after a month. However, participants used the proposed scheme to create passwords were better off in both a week's period and a month's period (see Figure 7.7). Pearson Chi-square analyses indicated that these results were significant both for a week's period (χ^2 (2, N=360) =10.131, p = .006) and for a month's period (χ^2 (2, N=360) = 17.963, p <.001).

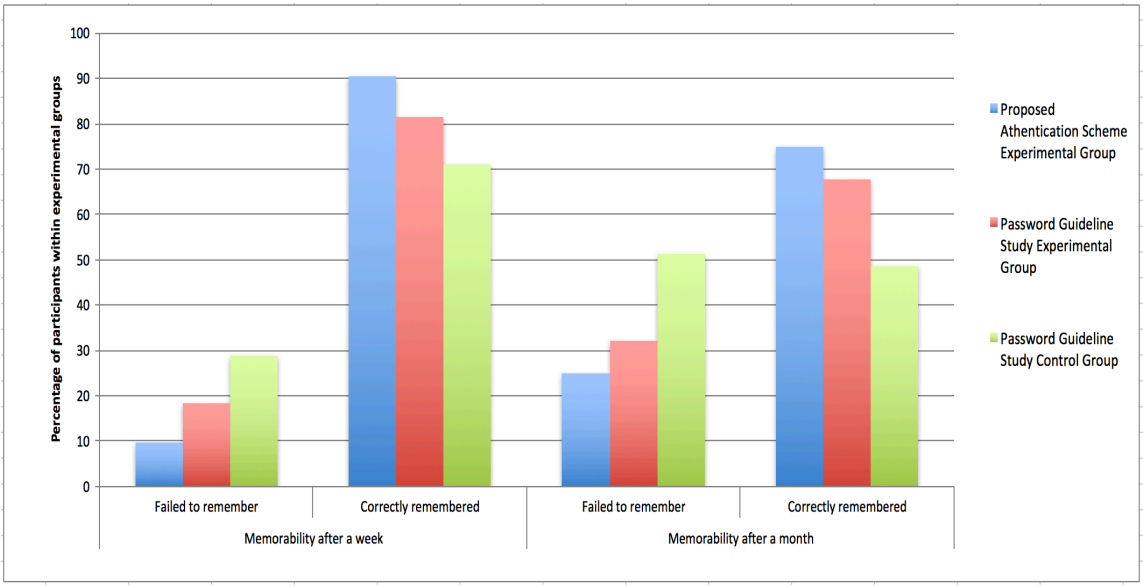


Figure 7. 7 Comparison of the memorability of the passwords created in the password guideline-advice study and proposed authentication scheme study

7.3.3.2 The Results Based on the Survey Responses

This section presents the results of the empirical study based on the participants' responses to questions.

User Satisfaction:

Participants were asked about their experiences on the use of the novel authentication scheme to create an account. 92 % of the participants liked the way of password creation with the scheme. 94 % of them considered that it was fun to use, and similarly, 90 % of the participants considered that the scheme was easy to use (see Figure 7.8). The questions of mini survey are presented in Appendix C.

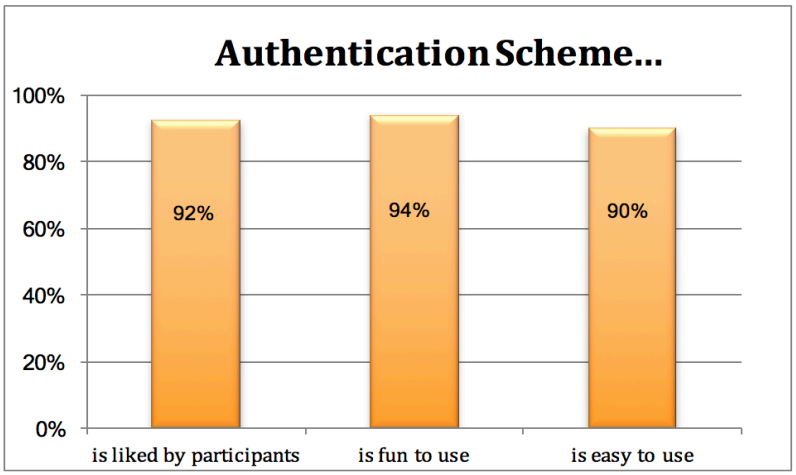


Figure 7. 8 Participants' opinion with regard to the use of the proposed scheme

When it comes to the beliefs of participants in the method used by the proposed authentication scheme, results showed that most participants agreed that this method created stronger passwords than other commonly used methods (89%). However, agreement was less on creating more memorable passwords with this method, though still more than half of the participants (58%) agreed that this method would create more memorable passwords. Figure 7.9 illustrates the participants' perception of the proposed scheme's ability to allow users to create strong and memorable passwords. However, results of the experiments showed that the actual memorability rates were higher than participants expected (refer to Figure 7.7).

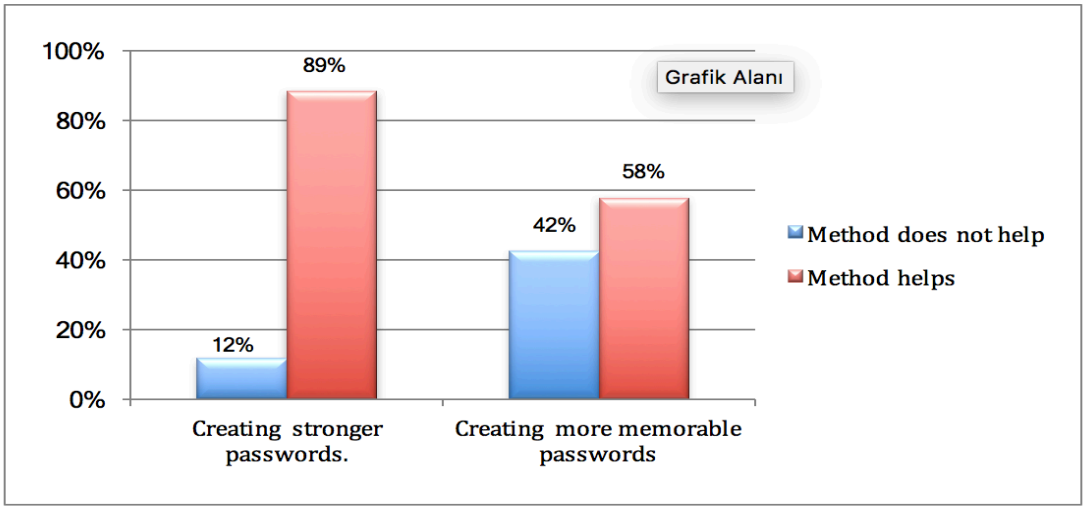


Figure 7. 9 Users perception of the proposed scheme's ability to produce strong and memorable passwords

In addition to the users' thoughts of the efficiency of the new authentication scheme on creating strong and memorable passwords, they were also asked whether they will prefer to use the scheme or not. As illustrated in Figure 7.10, only 5 out of 52 participants (9.6%) reported that they would not prefer to use the scheme neither for important passwords nor for others. On the other hand, 30 participants (32.7%) reported they would use the novel scheme for important passwords and 17 participants (57.7%) would use it for all passwords.

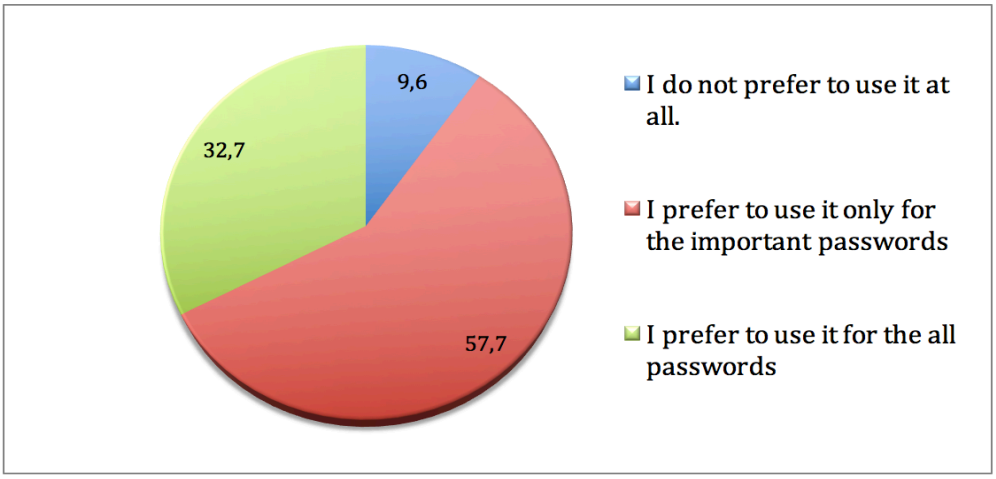


Figure 7. 10 User preferences on use of the proposed scheme

The empirical study yielded results that showed the proposed authentication scheme provides usability and security at the same time as well as high user satisfaction rates. Next chapter provides an overall discussion of the proposed design.

7.4 DISCUSSION

Traditional text passwords alone are vulnerable to brute-force and dictionary attacks as users choose weak and predictable passwords in favour of memorability. On the other hand, graphical passwords alone are subject to shoulder surfing attacks. They also introduce usability issues by making password creation process longer for users. For these reasons, a hybrid authentication scheme integrating text and recognition-based graphical passwords is proposed in this chapter. The design of the proposed scheme

differs from other combined schemes since it offers an integrated registration phase rather than two or three different steps. It largely preserves the sign in and log in experiences of users who are accustomed to use text passwords. The proposed scheme does not suggest a discrete graphical password creation step, instead it uses the images as cues to help users to create complex text passwords and memorize them easily. This also provides a usable authentication method by decreasing the steps of password verification. The proposed hybrid authentication method is implemented and an empirical study is conducted to evaluate its effectiveness on producing strong and memorable passwords.

The results of the empirical study which conducted to test the proposed scheme showed that this novel design provides an enjoyable user authentication experience ensuring usability and security at the same time. Probably the user-friendly design of the proposed authentication scheme brings about high user satisfaction.

It allows users to authenticate themselves in a similar way they do with conventional text-passwords, without increasing the registration time unreasonably. Considering the participants' first trial of a novel authentication system, the registration time is reasonable to create a password. There is not a significance difference between the login time of a traditional password scheme which mostly takes time to create passwords following the required password composition rules. The small difference with the registration and login time can be tolerated whereas the additional security is added to the scheme over the usual text password authentication. In the empirical study, the participants used the authentication scheme to log in only twice in a month. When this scheme is used for real systems, users' login times are likely to decrease in time as the frequency of logging into the system will be higher. As time goes by, users will also be able to memorize their passwords and will not need to resort to images to enter the characters.

Besides, it is an easy to use scheme and it helps users to create memorable as well as strong passwords which are resistant to dictionary attacks. Since the images in the registration phase are randomly placed in the portfolio every time, they include different characters for different users, and they are chosen by entering the characters under them through keyboard but not clicking on them provide a resistance to shoulder surfing attacks. It also provides a large password space by combining the text and images to create passwords. This reduces the possibility of cracking the passwords for third parties. The

results of the study showed that password cracking times are not reasonable to crack the passwords for a hacker. This demonstrates that the scheme is effective to eliminate brute-force and dictionary attacks.

It can be easily implemented in software alone which increases its chance to be deployed widely.

The results of this empirical study and the password guidelines-advice study are compared in the previous sections. The comparison of the results showed that the passwords created with the hybrid authentication scheme are stronger and more memorable than the passwords created by the participants in the experimental group of the password guidelines-advice study. However, the results of these studies should not be directly compared as various factors are different. The demographics, design, apparatus and procedure of the studies are different which could certainly affect the results. While the researcher has conducted this study in person, password guidelines-advice study was a web-based empirical study which participants completed the questionnaires online. The presence of the researcher could have had a big influence on the participants and affected the results.

7.5 SUMMARY

This chapter introduced the design and implementation of a novel hybrid password authentication scheme, combining the text and graphical password approach. The chapter also analysed and discussed the results of an empirical study conducted to evaluate the proposed scheme's effectiveness on producing strong and memorable passwords. The next chapter presents the overall discussion of the thesis and conclusions as well as the limitations of the study and future researches.

CHAPTER 8

DISCUSSION, CONCLUSION AND FUTURE WORK

8.1 INTRODUCTION

This chapter presents an overall discussion of this research study and conclusion of the empirical studies which have been conducted. It provides comments and suggestions about the research findings.

This chapter also discusses the contributions of this research to the password security field, and presents the possible future works and approaches for further investigation of usability and security issues which arise in password authentication by extending the findings of this research.

The next discussion part revisits and provides answers to four research questions which were set in the first chapter, guiding this research study.

8.2 DISCUSSION

This section provides the discussion of this thesis by providing answers to research questions which determines the aims and objectives of this research. The primary purpose of this research is proposing usable solutions to password security problem by considering the human factors problems. In accordance with this purpose, four research questions were determined on investigating human factors in knowledge-based password authentication. Since this thesis investigates both forms of knowledge-based authentication, the questions are also divided into two parts: The first two questions are related to traditional text password mechanisms, investigating the possible solutions to be used to improve users' password related behaviours. The first question is about whether persuasion strategies can be utilised to improve employees' motivation for adopting good password behaviours in organisations. The second research question particularly focuses on the efficiency of proposed password guideline supported by an encouraging text and several password creation tips on usability and security of password security. The next part of the thesis which aims to find solutions to two research questions is related to

graphical passwords. The questions in the second part examine the capability of graphical passwords to replace conventional text passwords, and effectiveness of a proposed novel hybrid authentication scheme integrating text and images.

The research questions are revisited and elaborated on by providing the critical analysis of the related empirical studies conducted as follows:

1- **"How can password related behaviours, which may potentially lead to security failures, be changed to improve overall password security in organisations?"**

The first questions investigated the reasons for employees' unwanted password-related behaviours undermining the information security in organisations, and the possible ways to motivate them to adopt good practices. An empirical study has been conducted with employees from different organisations to understand the reasons of their lack of motivation to behave in a secure manner particularly with regard to protecting their passwords. Results showed that most of the employees adopted coping strategies to handle the password problem in organisations. The cumbersome text password mechanisms including strict policy rules and poor designs of authentication schemes cause users to overlook the password security. Beside the usability issues of password mechanisms, employees' education and awareness level and, organisational factors such as workload also influence their password practices. The study showed that these influential factors vary in each organisation. The aim of the empirical study was first to identify these factors and then investigate the possible solutions to increase employees' motivation. Therefore, a questionnaire has been conducted with the employees who all access confidential information via passwords. Besides, IT specialists have been interviewed to determine the reasons of unsecure password behaviours. The IT specialists' perceptions on reasons of these behaviours did not seem to match the perceptions of employees who relatively have less computer / information security background. In most organisation, while employees blame the password schemes and policies they use, IT departments claimed that the most important reason of unsecure behaviours is employees' lack of education and awareness.

On the other hand, the results revealed the fact that there is a lack of motivation to protect passwords among the employees who are already educated about information

and password security. Therefore, the study also sought the possible methods to be applied by IT departments to improve employees' motivation to adopt secure password behaviours.

Based on the review of behaviour change theories and persuasion strategies, it seems that employees' can be convinced to protect their passwords and abandon coping strategies such as sharing passwords or selecting weak passwords. Efficiency of several persuasion strategies, social proof and authority principles of weapons of influence (Cialdini, 1988), reward and punishment and fear appeal has been evaluated through questionnaire and interviews including questions framed by these possible strategies. Also, a case study has been performed to test the effectiveness of these strategies with the selected company, a hospital which suffers information security flaws caused by employees' careless password behaviour. The empirical study sought to determine which persuasion strategies are more likely to result in influencing employees to adopt better password behaviours.

The results showed that the social proof and rewards and punishment strategies can be useful to improve employees' motivation in some organisations. However, it might be difficult to apply those strategies where the IT department is not able to monitor the employees' password practices all the time. The research also yielded results showing that the fear appeal is a significant motivation for most employees almost from all sectors. Finally, the authority principle seemed to be influential to raise awareness of password security among employees.

The study proves that some persuasion strategies can be utilised to improve users' security behaviour in organisations. However, there is not a guarantee that all strategies will work for all organisations. The strategies should be chosen carefully by security experts and IT specialists considering their applicability as well as the organisational / environmental factors and working conditions the employees confront. Also, the content of security training programs should be prepared particularly for each organisation taking all the influential factors into consideration. Since there are lots of variables affecting password security level in organisations such as organisational culture, password mechanisms used, password policy rules, environmental factors, the necessity and requirements of security differs for each of them. Therefore, the motivation strategies and training/awareness programs should be applied appropriately.

2- "To what extent can users be directed and motivated to choose strong passwords through password advice?"

Based on the results of the previous study conducted in this thesis and review of several studies by different researchers, it seems that users continue to select weak passwords despite the applied password policy rules. To evaluate the effect of strict password policy rules on password security, an empirical study has been conducted with university students. The study also seeks to examine the effectiveness of a proposed password guideline including a motivating message and several useful password creation tips on users' password preferences.

The participants were divided into two groups and each group is asked to login into a website. To create passwords to login into the websites they were provided with two different password guidelines. Participants in the control group were given common password creation rules, and the participants in the experimental group were given the proposed password guideline to create passwords. The results indicate that passwords created by the participants who receive the password guideline including a persuasive text and three password creation methods, are stronger and more memorable compared to the ones created by the participants in the control group who were asked to follow usual password creation rules. The text was telling them that they can create very strong and also memorable passwords by producing their own encryption formula as exampled by three methods in the guideline. These methods seem to be effective on inspiring users to create complex but memorable passwords. Also, the passwords created by the control group were more predictable and easier to crack than the experimental group's passwords.

This finding suggests that it is worth informing users that it is actually easy to create strong and memorable passwords via a message. The message was not only telling users what should they do to create better passwords but also showing them how to do with the simple example methods. As suggested previously, persuasion is an effective tool to motivate users to improve password security. The message in the proposed password guideline indeed coincides with the inherence of persuasion, which attempts to tackle the reluctance to motivate users to create better passwords.

The results show that strict password creation policies reduce the password security contrary to beliefs by causing users to create predictable passwords. With regards to the

password guidelines, it seems that persuasive message and password creation tips helped users to create better passwords. Therefore, this thesis suggests that these kinds of improvements should be done to existing password guidelines such as adding persuasive elements.

The studies conducted to answer the first two research questions provides interesting insights into possible measures to improve users' password behaviours as decreasing the use of coping strategies with passwords through persuasion strategies and increasing the strength and memorability of their passwords through effective password guidelines. Although motivating users to adopt better password behaviours through the persuasion approach, and improving the usability of existing text password mechanisms may seem practical, the vulnerability of text passwords remains an issue. Thus, the second part of this thesis focus on an alternative mechanism to the traditional text-based passwords: graphical passwords. Graphical passwords are also a form of knowledge based authentication which allows users to create their passwords using images and drawing lines instead of using letters, numbers or special characters.

As has been proposed as a promising alternative to traditional text passwords regarding memorability problem, graphical passwords have also some usability and security drawbacks. These are susceptible to several attacks including shoulder surfing, and they introduce usability issues by increasing the registration time. Thus, the next research question discusses whether graphical passwords are likely to replace text passwords.

3- "Can graphical passwords entirely replace the textual passwords?"

As known, text-based passwords are the most ubiquitous way of authentication. Users are accustomed to use them for many years despite its weaknesses. They are vulnerable to attacks since users often resort to coping strategies such as choosing weak passwords, writing them down and reusing or sharing them with other people. The length and complexity requirements of strong passwords causes the memorability problems and hence aforementioned coping strategies are adopted by users. Besides the memorability issue and vulnerability to brute-force and dictionary attacks, text passwords also face

other challenges such as phishing, social engineering and key-logging attacks.

The alternative authentication mechanisms have emerged due to the weaknesses of text passwords. such as graphical passwords. They were introduced due to the human memory's superiority to remember pictures and graphics over text and numbers. They indeed reduce the users' cognitive challenge; however, they also face several challenges.

Nevertheless, it is worth considering graphical passwords as an alternative mechanism since they are employed in two-factor authentication methods in combination with other authentication mechanisms to strengthen the security of critical accounts. Numerous academic research has been conducted by collaborating with security practitioners from industry, to improve the existing graphical password mechanism. However, the question of whether graphical password mechanism can replace the ubiquitous text-based authentication mechanism has not been answered yet.

There are several issues that need to be mentioned in relation to replacing moving traditional text passwords to the graphical passwords. First of all, it is not easy to convince users to move from using one technology which they are familiar with to another. Since, text passwords are the most common security mechanisms that users employ when confronted with any systems that require access control, it is rather difficult to change their routine to something completely new. If this new mechanism is totally different from the one to which they are more accustomed this is even more challenging. Users are generally reluctant to embrace new mechanisms if they already feel comfortable with the existing one. There have not been enough large scale studies conducted to investigate users' opinion of adopting new mechanism to understand their willingness. Only recently Vorster and Heerden (2015b) investigated user perceptions regarding graphical passwords. The survey they conducted showed that corporate users are not ready to adopt graphical passwords within organisations as more than half of the participants stated that they will not support the use of graphical passwords within their organisation. Majority of participants seemed to be apprehensive to use graphical passwords especially for financial transactions. These results revealed that users showed substantial resistance to the graphical password technology. However, there is a need for more academic study about users' perceptions regarding graphical passwords. Without such proper investigation, making assumption about the likelihood of graphical passwords replacing the text passwords is difficult.

Another issue which needs to be thought over is compatibility and adaptability of graphical passwords. Text passwords are widely used ranging from financial transactions to email accounts and social networking sites. It might be challenging to apply a new mechanism to all these systems. Although, in many cases text passwords have not been suitable to provide adequate security for some services especially for critical accounts, stakeholders mostly prefer to employ two factor (2F) authentications to improve security rather than changing the entire authentication mechanism to graphical passwords. This weakens the possibility of graphical passwords replacing the text password mechanism.

Affordability is another issue that should be reviewed to decide whether the change of authentication mechanism is really necessary. It appears that organisations have difficulty in deciding to change their existing password authentication mechanisms even though it risks potential password loss incidents. This is because the password loss can occur due to the many possibilities including the attacks through tricking users such as phishing, social engineering or key-logging attacks. Thus, organisations generally do not blame only the text password schemes to the extent that they need to be replaced with a new alternative mechanism such as graphical passwords (Zakaria, 2013). To make this decision, first reliable measurements should be carried out to determine the actual problem since the solution might not be easy or cheap all the time.

Finally, if the existing password mechanisms are considered problematic, then the proposed graphical passwords should be perfect to eliminate all the vulnerabilities of text passwords. However, it seems that most of the challenges facing text passwords are almost the same for graphical passwords, probably due to their similar nature of use and practice. Graphical passwords indeed are a promising alternative to conventional text passwords especially as a solution to the memorability problem, they suffer many vulnerabilities including the susceptibility to shoulder surfing attacks.

Despite that some security researchers insist upon promotion of alternative graphical password schemes; this thesis suggests that the problems of traditional text-based passwords can be solved with more efficient and easier ways than replacing by a totally new mechanism. Such solutions were investigated in this thesis, and the idea of adopting persuasion strategies is useful in terms of motivating users to behave in a secure manner thus decreasing the possibility of password security failures in organisation was found. This thesis also found that some improvement can be done to existing password

guidelines to provide users a secure and usable authentication experience. Such solutions require minimal cost to management in comparison with changing the entire existing authentication mechanism.

Considering the mentioned issues, this thesis propounds that graphical passwords are not likely to be a substitute for traditional text-based passwords in the near future. However, as they have some advantages over text-passwords, they can be used to strengthen the existing mechanisms such as in two-factor and (Passfaces, 2009) multi-factor authentication (Sabzevar, Stavrou, 2008) or hybrid password authentication mechanisms. Instead of new alternative graphical password proposals, this research suggests that there should be more efforts in finding solutions to improve the existing text password mechanisms. Therefore, a novel hybrid authentication scheme based on text and images was introduced and evaluated in this thesis. The next and final research question aims to answer to what extent can a hybrid scheme solve the password security and usability problem.

4- "Can a hybrid password authentication scheme integrating text and graphical passwords be solution to the password security and usability problems?"

Based on the previous discussion, the idea of improving text password authentication with the help of graphical passwords seems to be better than replacing text-based password authentication with graphical password authentication. This question investigates the efficiency of a proposed hybrid authentication scheme on improving security and usability of user-chosen passwords.

Authentication procedures are regarded as text passwords for the majority of computer users. However, they have well-known usability problems, especially in terms of memorability. As stated earlier, that human memory is able to remember pictures more easily than text and numbers is proven by many cognitive and psychological studies (Jermyn, 1999; Tao and Adams, 2008; Biddle, Chiasson and vanOorschot, 2011). As a result, various research has been conducted in both the security and human computer interaction (HCI) field in recent years to explore graphical passwords as an alternative or an enhancement, to text-based passwords.

The categorisation of graphical passwords and several schemes from each category were discussed in terms of their advantages as well as weaknesses in Chapter 5. The discussion shows that graphical passwords are far from being a perfectly secure and usable way of authentication since they are vulnerable to many attacks including brute force, guessing and observation attacks. Among others, shoulder surfing seems the main concerns against adopting graphical authentication in real use (Suo, Zhu, Owen, 2005). This is due to the nature of graphical passwords because while a user login system using a graphical password in a public place, their password can be stolen by another person who observes the user over their shoulder. In relation to this research, there are several shoulder defence mechanisms suggested by researchers to strengthen recognition-based graphical passwords. For example, Convex Hull Click (CHC) scheme developed by Sobrado and Birget (2002) used a huge number of pass-icons to confuse attackers to find the correct one. However, Man, Hong and Matthews (2003) proved that this scheme has some usability issues as so many objects which have to be fitted on screen seemed too small, making it difficult for users to distinguish between pass-objects and non-pass-objects Another possible technique to provide shoulder surfing resistance is Use Your Illusion (UYI) scheme (Hayashi, Christin, 2008) which displays degraded or distorted images in order to reduce the visibility of users' input.

On the other hand, the traditional text-based passwords are defended against shoulder surfing attacks by hiding passwords substituted by asterisks for the password characters in the display as the user logs in. However, their vulnerability to brute force and dictionary attacks due to the memorability problem is known, as mentioned in detail in this thesis. These indicate that text passwords and graphical passwords alone are subject to various attacks and, they also introduce usability problems. Therefore, a novel hybrid authentication scheme is proposed as a solution to the security and usability problems of both authentication mechanisms. The scheme integrates the text password with recognition based graphical passwords in a common registration and login phase in order to decrease the registration and login time. Basically, it is a text password scheme strengthened by recognition-based graphical passwords using images as cues to improve memorability of text password character. This is due to the fact that the human brain has better ability to remember images over texts. The implementation and evaluation of this proposed authentication scheme is presented in Chapter 6.

The scheme has many advantages such as resistance to brute-force and dictionary attacks since the passwords created with the hybrid scheme has a larger password space than text passwords in practice. It allows users to create complex, hard to crack passwords which contain different type of keyboard characters without including any meaningful details. The empirical study conducted to measure the strength and memorability of passwords created with the scheme showed that it indeed allowed participants to create stronger and more memorable passwords compared to traditional text-password schemes.

It also provides protection to shoulder surfing attacks allowing users to choose images by typing the characters placed beneath them into the password field rather than directly clicking on the images. After a while when users memorised the mixed complex password they would no longer need to look at the images so they can hide the image portfolios. This provides nearly perfect resistance to shoulder surfing attacks.

The login and sign in experience of users who are familiar with the text passwords are largely preserved. Probably because of this, user satisfaction rates were pretty high according the results of the questionnaire conducted to find out the users' opinions who tested the scheme. The scheme is also easy to implement in software which increases the chance of large-scale adoption in the internet.

Based on the results of the empirical study that evaluated the efficiency of proposed password scheme, it can substitute or coexist with traditional text-based password mechanisms without changing the existing user authentication profile. Thus, the scheme has potential to eliminate the weaknesses of conventional text password and graphical passwords by taking the advantages of both. As an answer to the final research question, the proposed hybrid password scheme can be a solution to many security and usability problems which arise in text-based and graphical-based password authentication.

The discussion of research questions has provided an overview of the security and usability issues and possible countermeasures in the knowledge based authentication domain. The next section presents contributions of this research to the password authentication field.

8.3 RESEARCH CONTRIBUTIONS

This thesis has made several contributions to the password security and usability field. The first part of the thesis presented solutions to improve traditional text-based password mechanisms. First, several persuasion strategies were utilised to improve password-related behaviour in organisations. The study revealed the fact that many organisations are in a position of suffering password security failures caused by user-behaviours but still do not apply user-centred solutions. However, with a few simple interventions, users can be motivated to abandon the behaviours which undermine the information security. To our knowledge, there is not much study that investigated the reasons for unsecure password practices in different organisations. The first empirical study has demonstrated that there is evidence to support the worthiness of applying persuasion strategies in different ways to improve employees' motivation to adopt secure password practices. The findings of this research can be extended by stakeholders to arrange compulsory training programs for employees before they are employed, and produce new information/password policy framed by persuasion strategies. These new regulations are applicable by organisations. They can take preventive countermeasures to password failures, if the appropriate persuasion strategies are applied. Briefly, this study can conduce to the use of persuasion strategies to motivate employees regarding password protection in order to avoid the loss of critical information. Thus, the findings of this study can be useful for influence strategists, password policy makers, IT specialists and password security practitioners.

Secondly, the first part of the thesis proposed a new password guideline including a motivating message and three sample password creation methods. The security and usability evaluation of the password guideline showed that these simple improvements to the usual password guidelines consisting of several password restriction rules make significant changes on strength and memorability of passwords. The proposed password guideline as a low-cost solution can contribute to a significant outcome in terms of improving the issues facing the text-based password authentication.

Results of these studies presented in the first part of the thesis, pointed out the importance of human factors that commonly receive little attention from security experts. This research focuses on human-factor issues in password authentication, and proposes user friendly solutions to these problems. Thus, this research also considers technical

solutions by introducing a novel hybrid password authentication scheme to increase resistance to brute-force, dictionary and shoulder surfing attacks in the second part of the thesis. The last empirical study has also produced empirical evidence to support the applicability of the proposed hybrid authentication scheme both from security and usability perspectives. The proposed scheme has been implemented and tested, the findings were promising to reduce existing, unsolved security and usability problems. In this research, all of the proposed countermeasures have been tested and evaluated in this thesis. They require minimal cost to be implemented, and take both theoretical and practical considerations into account.

This research does not claim to provide an ultimate solution to the existing issues which is in fact not possible where the human-factors are involved, but significantly contributes to the field. The findings create opportunity for interested parties to understand the insight behind the reasons for human-factor caused password problems, and it can be extended collaboratively to enhance the proposed solutions.

The next section provides some discussion on the limitations of the research undertaken and possible future work relevant to this research.

8.4 LIMITATIONS AND FUTURE RESEARCH

This research has some limitations and can be expanded with further studies. Thus, it creates some opportunities for future research to be conducted. With regards to the first study, a larger scale empirical study or experiment with more organisations recruiting more employees might be useful to draw more accurate conclusion about the efficiency of persuasion strategies on password security. Also, evaluating the effectiveness of other persuasion strategies on password security might be interesting.

Regarding password guideline/advice study, it will be interesting to add visual elements in password guideline to instruct users to create complex password. It would probably be useful to attract users' attention and make the password creation process more enjoyable. Also, implementing the proposed password guideline into different kinds of applications which require different levels of security, and conduct a further empirical study with different user groups, involving more participants would be useful. Moreover,

the literature on persuasion suggests that persuasion attempts are more likely to succeed if the persons are aware of the situation. Thus, adding some attributes to the password guideline informing users about possible attacks if they choose weak passwords might improve the compliance to password guideline.

With regards to improving the proposed hybrid password authentication, an immediate endeavour that can be carried out is to investigate whether the relation between the typed character with the first letters of the names of objects, famous people, activities etc. in images affects the security. These relations have been inspired by the Tip of the Tongue phenomenon in the hope of increasing the memorability of passwords. In the conducted user study, the majority of the participants indeed remembered correctly their passwords but yet it is difficult to say if this is caused by the association between the key passwords' characters and image portfolios. While expecting to increase usability, it might reduce the security by increasing the chance of shoulder surfing attacks. This is the dilemma of proposed scheme that need to be clarified so further investigations will be useful to find out the impact of associating typed characters with images on password security and memorability. This is an interesting research question as the challenge of balancing security and usability remains. It is also worthwhile making slight modifications on the scheme in order to increase usability. For example, the characters placed under the images can be changed each time even for the same user which means creating a one-time password each time. The security and usability evaluation of such scheme might yield interesting results.

The findings of all empirical studies conducted in this research study can be helpful and inspirational for other researchers to improve existing password mechanisms with further investigations.

8.5 SUMMARY

This final chapter provides a broad discussion of this research by revisiting each research questions. This chapter also highlights several contributions of this research, followed by limitations of the research and possible future work to be carried out.

REFERENCES

Aarons, G. A. (2006). Transformational and transactional leadership: Association with attitudes toward evidence-based practice. *Psychiatric services*, *57*(8), pp. 1162-1169.

Adams, A. and Sasse, M. (1999). Users are not the enemy. *Communications of the ACM*, 42(12).

Ajzen, I. (1988). *Attitudes, personality, and behaviour.* Milton-Keynes: Open University Press.

Ajzen, I. (1991). The Theory of Planned Behaviour. *Organizational Behaviour and Human Decision Processes,* 50, pp. 179-211.

Anderson, R. (1993). Why cryptosystems fail. In *Proceedings of the 1st ACM Conference on Computer and Communications Security*, pp. 215-227

Aviv, A.J., Gibson, K., Mossop, E., Blaze, M. and Smith, J. M. (2010). *Smudge attacks on smartphone touch screens.* In *Proceedings of the 4th USENIX conference on Offensive technologies,* pp.1-7.

Bada, M. and Sasse, A. (2014). Cyber Security Awareness Campaigns: Why do they fail to change behaviour?. Global Cyber Security Capacity Centre, University of Oxford, UK

Barton, B. F. and Barton, M. S. (1984). User-friendly password methods for computer-mediated information systems. *Computers & Security*, *3*(3), pp. 186-195.

Beautement, A., Becker, I., Parkin, S., Krol, K. and Sasse, A. (2016). Productive security: A scalable methodology for analysing employee security behaviours. In *Symposium on Usable Privacy and Security (SOUPS 2016)*, pp. 253–270.

Bekkering, E., Warkentin, M. and Davis, K. (2003). A longitudinal comparison of four password procedures. In *Proceedings of the 2003 Hawaii International Conference on Business*, Honolulu, HI, June.

Bellovin, S. M. and Merritt, M. (1992). Encrypted key exchange: Password-based protocols secure against dictionary attacks. In *Research in Security and Privacy, IEEE* pp. 72-84.

Ben-Asher, N., Kirschnick, N., Sieger, H., Meyer, J., Ben-Oved, A. and Moller, S., (2011), On the need for different security methods on mobile phones, In *Proceedings of the 13th International Conference on Human Computer Interaction with Mobile Devices and Services*, ACM, pp. 465–473.

Bensinger, D., (1998), *Human memory and the graphical password*, Passlogix, White Paper.

Bettinghaus, E. P. and Cody, M. J. (1987). *Persuasive Communication* (4th ed.), Holt, Rinehart & Winston, New York: NY.

Bhanushali, A., Mange, B., Vyas, H., Bhanushali, H., & Bhogle, P. (2015). Comparison of Graphical Password Authentication Techniques. *International Journal of Computer Applications*, *116*(1).

Biddle, R., Chiasson, S. and van Oorschot, P. C. (2012). Graphical passwords: Learning from the first twelve years. *ACM Computing Surveys (CSUR)*, *44*(4), p. 19.

Bishop, M. and Klein, D. V. (1995). Improving system security via proactive password checking. *Computers & Security*, *14*(3), pp. 233-249.

Blonder, G. (1996). *Graphical Passwords*, United States Patent 5559961

Bond, M. (2008). Comments on grIDsure authentication. *Online at http://www. cl. cam. ac. uk/~ mkb23/research/GridsureComments. pdf*.

Bonneau, J., Herley, C., van Oorschot, P. C. and Stajano, F. (2012). The quest to replace passwords: A framework for comparative evaluation of web authentication schemes. In *Security & Privacy (SP), IEEE Symposium,* pp. 553-567.

Boujettif, M. and Wang, Y. (2010). Constructivist approach to information security awareness in the middle east. In *Broadband, Wireless Computing, Communication and Applications (BWCCA), International Conference,* IEEE, pp. 192-199.

Briggs, P. and Olivier, P. L. (2008). Biometric Daemons: Authentication via electronic pets. In Proceedings of the Conference on Human Factors in Computing Systems (CHI'08), ACM, pp. 2423-2432.

Brostoff, A. (2004). *Improving Password System Effectiveness,* PhD Dissertation, Department of Computer Science University College London.

Brostoff, S. and Sasse, M. A. (2000). Are Passfaces more usable than passwords? A field trial investigation. In *People and Computers XIV-Usability or Else!,* Springer London, pp. 405-424.

Brostoff, S., Inglesant, P. and Sasse, M. (2010). Evaluating the usability and security of a graphical one-time pin system. In *Proceedings of the 24th BCS Interaction Specialist Group Conference*. British Computer Society, pp. 88-97

Brown, A. S. (1991). A review of the tip-of-the-tongue experience. *Psychological bulletin*, *109*(2), pp 204.

Brown, R. and McNeill, D. (1966). The "tip of the tongue" phenomenon. *Journal of verbal learning and verbal behaviour*, *5*(4), pp. 325-337.

Burger, J. M., Messian, N., Patel, S., Del Prado, A. and Anderson, C. (2004). What a Coincidence! The Effects of Incidental Similarity On Compliance. *Personality and Social Psychology Bulletin,* 30, pp. 35-43.

Burnett, M., and Kleiman. D. (2006) ed. *Perfect Passwords*. Rockland, MA: Syngress Publishing, ISBN 1-59749-041-5, p. 181.

Burr, W., Dodson, D. and Polk, W. (2006). Electronic authentication guideline. Technical report, National Institute of Standards and Technology (NIST), Special Publication 800-63 Version 1.0.2.

Callas, J., Donnerhacke, L., Finney, H., Shaw, D. and Thayer, R. (2007). *OpenPGP message format,* Technical Report (No. RFC 4880).

Campbell, J., Ma, W. and Kleeman, D. (2006). Password Composition Policy: Does Enforcement Lead to Better Password Choices. In *Proceedings of The 17th Australian Conference on Information Systems*, pp. 60-69.

Carstens, D. S., Malone, L. C. ans McCauley-Bell, P. (2006). Applying chunking theory in organizational password guidelines. *Journal of Information, Information Technology, and Organizations*, *1*, pp. 97-113.

Carstens, D. S., McCauley-Bell, P. R., Malone, L. C. and DeMara, R. F. (2004). Evaluation of the human impact of password authentication practices on information security. *Information Science Journal, 7*, pp. 67-85.

Castelluccia, C., Duermuth, M. and Perito, D. (2012). Adaptive Password-Strength Meters from Markov Models. In *Network and Distributed System Security Symposium* (*NDSS)*, ISOC.

Cerná, M. and Poulová, P. (2009). User testing of language educational portals. *E+ M Economics and management*, (3), pp. 104-117.

Chadwick, D. (1999). Smart Cards aren't always the Smart Choice. *Computer*, *32*(12), pp. 142-143.

Chen, Y.L., Ku, W.C, Yeh, Y.C and Liao, D.M. (2013). A simple text-based shoulder surfing resistant graphical password scheme. *IEEE 2nd International Symposium on Next Generation Electronics,* pp. 161-164.

Cheswick, W. (2012). Rethinking passwords. *Queue*, *10*(12), p. 50.

Chiasson, S., Biddle, R. and van Oorschot, P. C. (2007). A second look at the usability of click-based graphical passwords. In *Proceedings of the 3rd Symposium on Usable Privacy and Security,* ACM, pp. 1-12.

Chiasson, S., Forget, A., Biddle, R. and van Oorschot, P. C. (2008). Influencing users towards better passwords: persuasive cued click-points. In *Proceedings of the 22nd British HCI Group Annual Conference on People and Computers: Culture, Creativity, Interaction, 1,* pp. 121-130.

Chiasson, S., Forget, A., Biddle, R. and van Oorschot, P. C. (2009a). User interface design affects security: Patterns in click-based graphical passwords. *International Journal of Information Security*, *8*(6), pp. 387-398.

Chiasson, S., Forget, A., Stobert, E., van Oorschot, P. and Biddle, R. (2009b). Multiple password interference in text and click-based graphical passwords. *ACM Computer and Communications Security (CCS)*.

Chiasson, S., Stobert, E., Forget, A., Biddle, R. and Van Oorschot, P. C. (2012). Persuasive cued click-points: Design, implementation, and evaluation of a knowledge-based authentication mechanism. *IEEE Transactions on Dependable and Secure Computing*, *9*(2), pp. 222-235.

Chiasson, S., van Oorschot, P. C. and Biddle, R. (2006). A Usability Study and Critique of Two Password Managers. In *Usenix Security*. 6.

Chiasson, S., van Oorschot, P. C. And Biddle, R. (2007). Graphical password authentication using cued click points. In *European Symposium on Research in Computer Security*, Springer Berlin Heidelberg, pp. 359-374.

Cialdini, R. B. (1988). *Influence Science and Practice* (2nd ed.), Pearson, Boston.

Cialdini, R. B. (2001). Harnessing the science of persuasion, *Harvard Business Review*, *79*(9), pp. 72-81.

Cialdini, R. B. (2005). Don't throw in the towel: Use social influence research. *American Psychological Society Observer*, 18(4), pp. 33-34.

Clair, L. S., Johansen, L., Enck, W., Pirretti, M., Traynor, P., McDaniel, P. and Jaeger, T. (2006). Password exhaustion: Predicting the end of password usefulness. In *International Conference on Information Systems Security*, Springer Berlin Heidelberg, pp. 37-55.

Clarke, N. L. and Furnell, S. M. (2005). Authentication of users on mobile telephones–A survey of attitudes and practices. *Computers & Security*, *24*(7), pp. 519-527.

Collider, S. (2016). *How Secure Is My Password?*. [online] Howsecureismypassword.net. Available at: https://howsecureismypassword.net [Accessed 14 Jan. 2017].

Coventry, L., Briggs, P., Blythe, J. and Tran, M. (2014). Using behavioural insights to improve the public's use of cyber security best practices. *gov.uk report*, Government Office for Science, London, UK.

Cowan, N. (2001). The magical number 4 in short-term memory: A reconsideration of mental storage capacity. *Behavioral and Brain Sciences*, 24(1).

Cranor, L. F. (2008). A Framework for Reasoning About the Human in the Loop, In *Proceedings of The 1st Conference on Usability, Psychology and Security*, 8(2008), pp. 1-15.

Cranor, L. F. and Garfinkel, S. (2005). Security and usability: designing secure systems that people can use, *O'Reilly Media, Inc*., pp. 175-197.

Crystal, D. (2011). *Dictionary of linguistics and phonetics* (Vol. 30). John Wiley & Sons.

Das, A., Bonneau, J., Caesar, M., Borisov, N. and Wang, X. (2014). The Tangled Web of Password Reuse. In *NDSS*, 14, pp. 23-26.

Davis, D., Monrose, F., and Reiter, M. (2004). On User Choice in Graphical Password Schemes, In *Proceedings of The 13th USENIX Security Symposium,* San Diego, CA, USA, USENIX Association, pp. 151-164.

De Angeli, A., Coutts, M., Coventry, L., Johnson, G. I., Cameron, D. and Fischer, M. H. (2002). VIP: a visual approach to user authentication. In *Proceedings of the working conference on advanced visual interfaces*, ACM, pp. 316-323.

Deshmukh, P. D. S. M. and Pawar, A. B. (2013). Persuasive Cued Click Points with click draw based graphical password scheme. *International Journal of Soft Computing and Engineering (IJSCE) ISSN*, pp. 2231-2307.

Dhamija, R., and Perrig, A. (2000). Deja Vu: A User Study Using Images for Authentication. In *Proceedings of The 9th Conference on USENIX Security Symposium*, Denver, Colorado, US, August, pp.14-17

Dunphy, P. and Yan, J., (2007), *Do Background Images Improve "Draw A Secret" Graphical Passwords,* In Proceedings of *The 14th ACM Conference on Computer and*

Communications Security, Alexandria, VA, US, Oct 29-Nov 2, ACM Press New York, NY, USA, pp.36-47

Encyclopedia.com. (2004). *Tip-of-the-Tongue Phenomenon - Dictionary definition of Tip-of-the-Tongue Phenomenon | Encyclopedia.com: FREE online dictionary*. [online] Available at: http://www.encyclopedia.com/psychology/encyclopedias-almanacs-transcripts-and-maps/tip-tongue-phenomenon [Accessed 9 Nov. 2016].

Evans Jr, A., Kantrowitz, W. and Weiss, E. (1974). A user authentication scheme not requiring secrecy in the computer. *Communications of the ACM*, *17*(8), pp. 437-442.

Everitt, K. M., Bragin, T., Fogarty, J. and Kohno, T. (2009). A comprehensive study of frequency, interference, and training of multiple graphical passwords. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* ACM, pp. 889-898.

Fazio, R. H., Powell, M. C. and Williams, C. J. (1989). The Role of Attitude Accessibility in The Attitude-to-Behaviour Process. *Journal of Consumer Research,* 16, pp. 280-288.

Federal Information Processing Standards (FIPS), (1985). *Password usage*. [online] Available at: https://www.hsdl.org/?view&did=440923 [Accessed 10 Jun. 2014].

Finjan Blog. (2016). *Password Attacks - How They Occur and How to Guard Against Them*. [online] Available at: https://blog.finjan.com/password-attacks-how-they-occur-and-how-to-guard-against-them/ [Accessed 10 Oct. 2017]

Fishbein, M. and Ajzen, I. (1975), *Belief, Attitude, Intention and Behaviour: An Introduction to Theory and Research*. Addison Wesley, Reading: MA, USA.

Florencio, D. and Herley, C. (2007). A Large-Scale Study of Web Password Habits, In *Proceedings of The 16th International Conference on World Wide Web*, ACM, pp. 657-666.

Florencio, D., Herley, C. and Coskun, B. (2007). Do strong web passwords accomplish anything?. In *Workshop on Hot Topics in Security (HotSec). USENIX, 7*(6).

Florencio, D., Herley, C. and van Oorschot, P. C. (2014). Password portfolios and the finite-effort user: Sustainably managing large numbers of accounts. In *Proc. USENIX Security,* pp. 575-590.

Fogg, B. J. (1998). Persuasive Computers: Perspectives and Research Direction. In *Proceedings of the Conference on Human Factors in Computing Systems*, ACM Press/Addison - Wesley Publishing Co., pp. 225-232.

Fogg, B. J. (2002). Persuasive technology: Using Computers to Change What We think and Do. *Ubiquity*, 5.

Forget, A., Chiasson, S., van Oorschot, P. C. and Biddle, R. (2008). Improving text passwords through persuasion. In *Proceedings of the 4th symposium on Usable privacy and security*, ACM, pp. 1-12.

Forget. A. (2012). *A world with many authentication schemes*. Ph.D., Carleton University.

Furnell, S. (2007). An assessment of website password practices. *Computers & Security*, *26*(7), pp. 445-451.

Garrison, C. P. (2008). An evaluation of passwords. *The CPA Journal*, *78*(5), p. 70.

Gass, R. H. and Seiter, J. S. (2015). *Persuasion: Social influence and compliance gaining*. Routledge.

Gaw, S. and Felten, E. W. (2006). Password management strategies for online accounts. In *Proceedings of the second symposium on Usable privacy and security*, ACM, pp. 44-55.

Goldberg, J., Hagman, J. and Sazawal, V. (2002). Doodling our way to better authentication, In *CHI Extended Abstracts on Human Factors in Computing Systems*, ACM, pp. 868-869.

Grawmeyer, B. and Johnson, H. (2011). Using Multiple Password: A Week to a View. *Interacting with Computers, 23*(3), pp. 256-267.

Hadyn, D. E., Bruce, V., De Schonen, S. (1992). *The Development of Face Processing Skills*. Philosophical Transactions: Biological Sciences, (335), pp. 105 -111

Haga, W. J. and Zviran, M. (1991). Question-and-answer passwords: An empirical evaluation. *Information Systems*, *16*(3), pp. 335-343.

Haque, M. A. and Babbar Imam, N. A. (2012). 2-Round Hybrid Password Scheme. *International Journal of Computer Engineering and Technology (IJCET)*, *3*(2), pp. 579-587.

Haque, M. A. and Imam, B. (2014). A New Graphical Password: Combination of Recall & Recognition Based Approach. *World Academy of Science, Engineering and Technology, International Journal of Computer, Electrical, Automation, Control and Information Engineering*, *8*(2), pp. 320-324.

Hayashi, E. and Hong, J. (2011). A diary study of password usage in daily life. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems,* ACM*,* pp. 2627-2630.

Hayashi, E. and Christin, N. (2008). *Use Your Illusion: Secure Authentication Usable Anywhere*. In Proceedings of *The 4th Symposium on Usable Privacy and Security*, ACMPress New York, NY, USA, pp. 35-45.

Herath, T. and Rao, H. R. (2009). Protection Motivation and Deterrence: A Framework for Security Policy Compliance in Organisations, *European Journal of Information Systems,* 18, pp. 106-125.

Herley, C. and van Oorschot, P. C. (2012). A research agenda acknowledging the persistence of passwords. *IEEE Security & Privacy*, *10*(1), pp. 28-36.

Herley, C., van Oorschot, P.C. and Patrick, A. S. (2009). Passwords: If We're So Smart, Why Are We Still Using Them?. In *Proceedings of The 13th International Conference on Financial Cryptography & Data Security*, Springer-Berlin Heidelberg, pp. 230-237.

Hoonakker, P., Bornoe, N. and Carayon, P. (2009). Password Authentication from Human Factors Perspective: Results of a Survey among End-Users, In *Proceedings of The 53rd Annual Meeting of the Human Factors and Ergonomics Society*, pp. 459-463.

Hub, M., Čapek, J., & Myšková, R. (2011). Relationship between security and usability–authentication case study.

Humaidi, N. and Balakrishnan, V. (2012). The Influence of Security Awareness and Security Technology on Users' Behavior towards the Implementation of Health Information System: A Conceptual Framework. In *2nd International Conference on Management and Artificial Intelligence IPEDR*, 35, pp. 1-6.

Inglesant, P. G. and Sasse, M. A. (2010). The true cost of unusable password policies: password use in the wild. In *Proceedings of the 28th international conference on Human factors in Computing Systems*, ACM, pp. 383-392.

Ives, B., Walsh, K. R. and Schneider, H. (2004). The domino effect of password reuse. *Communications of the ACM*, *47*(4), pp. 75-78.

Jablon, D. P. (1996). Strong password-only authenticated key exchange. *ACM SIGCOMM Computer Communication Review*, *26*(5), pp. 5-26.

Jain, A. K., Ross, A. and Pankanti, S. (2006). Biometrics: a tool for information security. *IEEE transactions on information forensics and security*, *1*(2), pp. 125-143.

Jermyn, I., Mayer, A., Monrose, F., Reiter, M. and Rubin, A. (1999). The Design and Analysis of Graphical Passwords, *Proceedings of the 8th USENIX Security Symposium*, Washington DC, pp. 1-14.

Jeyaraman, S. and Topkara, U. (2005). Have the cake and eat it too-Infusing usability into text-password based authentication systems. In *Computer Security Applications Conference,* pp. 10.

Johnston, A. C. and Warkentin, M. (2010). Fear Appeals and Information Security Behaviours: An Empirical Study, *MIS Quarterly,* 34(3), pp. 549-566.

Just, M. (2003). Designing secure yet usable credential recovery systems with challenge questions. In *CHI Workshop on Human-Computer Interaction and security systems, Ft Lauderdale*, pp. 1-6.

Just, M. (2004). Designing and evaluating challenge-question systems. *IEEE Security & Privacy*, *2*(5), pp. 32-39.

Just, M. and Aspinall, D. (2009). Personal choice and challenge questions: a security and usability assessment. In *Proceedings of the 5th Symposium on Usable Privacy and Security* ACM, p. 8.

Just, M. and Aspinall, D. (2010). Challenging challenge questions: an experimental analysis of authentication technologies and user behaviour. *Policy & Internet*, *2*(1), pp. 99-115.

Karlins, M. and Abelson, H. I. (1970). *Persuasion: How Opinions and Attitudes Are Changed* (2nd ed.), Springer Publishing Company, New York.

Kaushal, S. (2011). Effect of leadership and organizational culture on information technology effectiveness: A review. In *Research and Innovation in Information Systems (ICRIIS), International Conference,* IEEE, pp. 1-5.

Keith, M., Shao, B. and Steinbart, P. J. (2007). The usability of passphrases for authentication: An empirical field study. *International journal of human-computer studies*, *65*(1), pp. 17-28.

Kelley, P. G., Komanduri, S., Mazurek, M. L., Shay, R., Vidas, T., Bauer, L., Christin, N., Cranor, L. and Lopez, J. (2012). Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *Security and Privacy, IEEE Symposium,* pp. 523-537.

Kirlappos, I. and Sasse, M. A. (2012). Security Education against Phishing: A Modest Proposal for a Major Rethink. *IEEE Security and Privacy Magazine* 10(2), pp. 24-32.

Kirlappos, I., Parkin, S. and Sasse, M. A. (2014). Learning from "Shadow Security": Why understanding non-compliance provides the basis for effective security. *Workshop on Usable SecurityKreuter, M. W., & McClure, S. M. The role of culture in health communication. Annual Review of Public Health*, 25, pp. 439-455.

Klein, D. V. (1990). Foiling the cracker: A survey of, and improvements to, password security. In *Proceedings of the 2nd USENIX Security Workshop*, pp. 5-14.

Komanduri, S., Shay, R., Kelly, P. G., Mazurek, M. L., Bauer, L., Christin, N. and Egelman, S. (2011). Of Passwords and People: Measuring the Effect of Password-Composition Policies. In *Proceedings of the Human Factors and Computing Systems*, ACM, pp. 2595-2604.

Koskosas, I., Kakoulidis, K. and Siomos, C. (2011). Examining the linkage between information security and end-user trust. *International Journal of Computer Science & Information Security,* 9, pp. 21-31.

Kotadia, M. (2004). *Gates predicts death of the password*. [online] CNET. Available at: https://www.cnet.com/news/gates-predicts-death-of-the-password/ [Accessed 10 May 2014].

Kreicberge, L. (2010). Internal threat to information security countermeasures and human factor with SME. *Business Administration and Social Sciences*, Lulea University of Technology, pp. 1-66.

Kukkonen, O. H. and Harjumaa, M. (2008). Towards Deeper Understanding of Persuasion in Software and Information Systems. In *Proceedings of the First International Conference on Advances in Computer-Human Interaction*, IEEE, pp. 200-205.

Kuo, C., Romanosky, S. and Cranor, L. F. (2006). Human selection of mnemonic phrase-based passwords. In *Proceedings of the second symposium on Usable privacy and security,* ACM, pp. 67-78.

Lamport, L. (1981). Password authentication with insecure communication. *Communications of the ACM*, *24*(11), pp. 770-772.

Leach, J. (2003). Improving user security behaviour. *Computers & Security*, *22*(8), pp. 685-692.

Lo, M. C., Ramayah, T. and De Run, E. C. (2010). Does transformational leadership style foster commitment to change?. The case of higher education in Malaysia. *Procedia-Social and Behavioural Sciences*, 2(2), pp. 5384-5388.

Lord, N. (2017). *What is a Phishing Attack? Defining and Identifying Different Types of*

Phishing Attacks. [online] Digital Guardian. Available at: https://digitalguardian.com/blog/what-phishing-attack-defining-and-identifying-different-types-phishing-attacks [Accessed 2 Feb. 2017].

Man, S., Hong, D. and Matthews, M. M. (2003). A Shoulder-Surfing Resistant Graphical Password Scheme-WIW. In *Security and Management*, pp. 105-111.

Manning, C. D. and Schutze, H. (1999). *Foundations of statistical natural language processing* (Vol. 999). Cambridge: MIT press.

Martin, N., and Rice, J. (2011). Cybercrime: Understanding and addressing the concerns of stakeholders. *Computers & Security,* 30, pp. 803-814.

Mathew, G. and Thomas, S. (2013). A Novel Multifactor Authentication System Ensuring Usability and Security. *arXiv preprint arXiv:1311.4037*.

Milgram, S. (1974). *Obedience to Authority: An Experimental View*. New York: Harper & Row.

Miller, G. A. (1956). The magical number seven, plus or minus two: some limits on our capacity for processing information. *Psychological review*, *63*(2), p. 81.

Miller, G. R. (1980). On Being Persuaded: Some Basic Distinctions. In *Persuasion: New Directions in Theory and Research*, M. E. Roloff & G. R. Miller, Ed., Sage, Beverly Hills: California, pp. 11-28.

Mokal, P. H. and Devikar, R. N. (2014). A Survey on Shoulder Surfing Resistant Text Based Graphical Password Schemes. *International Journal of Science and Research (IJSR)*, *3(4)*, pp. 747-750.

Moncur, W. and Leplâtre, G. (2007). Pictures at the ATM: exploring the usability of multiple graphical passwords. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 887-894.

Morris, R. and Thompson, K. (1979). Password security: A case history. *Communications of the ACM*, *22*(11), pp. 594-597.

Nali, D. and Thorpe, J. (2004). Analyzing user choice in graphical passwords. *School of Computer Science, Carleton University, Tech. Rep. TR-04-01*.

Neuman, C., Hartman, S., Yu, T. and Raeburn, K. (2005). The Kerberos network authentication service (V5), Technical Report (No.RFC 4120).

Nithyanand, R. and Johnson, R. (2013). The password allocation problem: Strategies for reusing passwords effectively. In *Proceedings of the 12th ACM workshop on Workshop on privacy in the electronic society*, ACM, pp. 255-260.

Norman, D. (1988). *The Design of Everyday Things*, Basic Books

O'Gorman, L. (2003). Comparing passwords, tokens, and biometrics for user authentication. *Proceedings of the IEEE*, *91*(12), pp. 2021-2040.

O'Keefe, D. J. (1990). *Persuasion: Theory and Research*. Sage, New Park: California.

Openwall.com. (n.d.). *John the Ripper password cracker*. [online] Available at: http://www.openwall.com/john/ [Accessed 20 Sep. 2015].

Passfaces (2009). *The Science Behind Passfaces*. [online] Available at: http://www.passfaces.com/published/The%20Science%20Behind%20Passfaces.pdf [Accessed 15 Aug. 2015].

Passwordmeter.com. (n.d.). *Password Strength Checker*. [online] Available at: http://www.passwordmeter.com [Accessed 5 Jan. 2017].

Patrick, A. S. (2008). Monitoring corporate password sharing using social network analysis. In *International Sunbelt Social Network Conference*.

Patterson, K., Grenny, J., Maxfield, D., McMillan, R. and Switzler, A. (2008). *Influencer, the power to change anything*. McGraw-Hill Professional.

Patterson, K., Grenny, J., Maxfield, D., McMillan, R. and Switzler, A. (2011). *Change anything: the new science of personal success*. Hachette, UK.

Perloff, R. M. (2010). *The Dynamics of Persuasion: Communication and Attitudes in the 21st Century*, 2nd ed., Lawrence Erlbaum Associates, Publisher, Mahwah, New Jersey.

Perloff, R. M. (2016). *The Dynamics of Persuasion.* 1st ed. Milton*:* Taylor and Francis

Piazzalunga, U., Salvaneschi, P., and Coffetti, P. (2005). The usability of security devices. *Security and usability: designing secure systems that people can use*, O'Reilly Media, Inc., pp. 221-242.

Polanski, T. (n.d.). *Dr. Robert Cialdini and 6 principles of persuasion*. [online] Available at: https://www.influenceatwork.com/wpcontent/uploads/2012/02/E_Brand_principles.pdf [Accessed 9 Oct. 2016].

Posey, C., Roberts, T. L. and Lowry, P. B. (2015). The impact of organizational commitment on insiders' motivation to protect organizational information assets. *Journal of Management Information Systems*, *32*(4), pp. 179-214.

Posey, C., Roberts, T., Lowry, P. B., Courtney, J. and Bennett, B. (2011). Motivating the insider to protect organizational information assets: evidence from protection motivation theory and rival explanations.

Proctor, R. W., Lien, M. C., Vu, K. P. L., Schultz, E. E. and Salvendy, G. (2002). Improving computer security for authentication of users: Influence of proactive password restrictions. *Behavior Research Methods*, *34*(2), pp.163-169.

Rabkin, A. (2008). Personal knowledge questions for fall-back authentication: Security questions in the era of Facebook. In *Proceedings of the 4th symposium on Usable privacy and security,* ACM, pp. 13-23.

Ramesh V., Venkatesvarlu P., Raju, S. (2015). A New Authentication Mechanism Based on Graphical Password. *International Journal&Magazine of Engineering, Technology, Management and Research, A Peer Reviewed Open Access International Journal, 2(4).*

Rao, K. and Yalamanchili, S. (2012). Novel shoulder-surfing resistant authentication schemes using text-graphical passwords. *International Journal of Information and Network Security*, *1*(3), pp.163-170.

Reason, J. (1990). *Human Error*, Cambridge, UK: Cambridge University Press.

Renaud, K. (2003). Quantifying the Quality of Web Authentication Mechanisms. A Usability Perspective. *Journal of Web Engineering*, Rinton Press, pp. 1-29

Renaud, K. (2005). Evaluating authentication mechanisms. *Security and usability*: *designing secure systems that people can use,* O'Reilly Media, Inc., pp. 103-128.

Renaud, K. and De Angeli, A. (2009). Visual passwords: cure-all or snake-oil?. *Communications of the ACM*, 52(12), pp. 135-140.

Renaud, K., Mayer, P., Volkamer, M. and Maguire, J. (2013). Are graphical authentication mechanisms as strong as passwords?. In *Computer Science and Information Systems (FedCSIS),* IEEE, pp. 837-844.

Rogers, R.W. (1975). A Protection Motivation Theory of Fear and Attitude Change. *Journal of Psychology,* 91, pp. 93-114.

Rogers, R.W. (1983). Cognitive and Physiological Process in Fear Appeals and Attitude Change: A Revised Theory of Protection Motivation. *Social Psychophysiology*, New York: Guilford Press, pp. 153-176

Rogers, Y., Sharp, H., and Preece, J. (2011). Interaction design: beyond human computer interaction, 2 ed. John Wiley and Sons.

Sabzevar, A. P. and Stavrou, A. (2008). Universal Multi-Factor Authentication Using Graphical Passwords. In *Proceedings of The 2008 IEEE International Conference on Signal Image Technology and Internet Based Systems*, IEEE Computer Society, pp. 625-632.

Sasse, M. A., Brostoff, S. and Weirich, D. (2001). Transforming The 'Weakest Link' - A Human/Computer Interaction Approach to Usable Security and Effective Security, *BT Technology Journal, 19*(3), pp. 122-131.

Schechter, S., Brush, A. B. and Egelman, S. (2009). It's no secret. Measuring the security and reliability of authentication via “secret” questions. In *Security and PrivacY IEEE Symposium,* pp.375-390.

Schechter, S., Herley, C. and Mitzenmacher, M. (2010). Popularity is everything: A new

approach to protecting passwords from statistical-guessing attacks. In *Proceedings of the 5th USENIX conference on Hot topics in security*, USENIX Association, pp. 1-8.

Schneier, B. (2004). *Secrets and lies: digital security in a networked world*. John Wiley & Sons.

Schultz, E. E., Proctor, R. W., Lien, M.-C. and Savendy, G. (2001). Usability and Security: An Appraisal of Usability Issues in Information Security Methods, *Computers and Security 20*(7), pp. 620-634.

Schwartz, B. L. and Metcalfe, J. (2011). Tip-of-the-tongue (TOT) states: Retrieval, behaviour, and experience. *Memory & Cognition*, *39*(5), pp. 737-749.

Shannon, C. E. (1951). Prediction and entropy of printed English. *Bell Labs Technical Journal*, *30*(1), pp. 50-64.

Shay, R., Kelley, P., Komanduri, S., Mazurek, M., B. Ur, Vidas, T., Bauer, L., Christin, N. and Cranor, L. (2011). Correct horse battery staple: Exploring the usability of system-assigned passphrases. In *Proceedings of the eighth symposium on usable privacy and security,* ACM, p. 7.

Shay, R., Komanduri, S., Kelly, P. G., Leon, P. G., Mazurek, M. L., Bauer, L. and Cranor, L. F. (2010). Encountering Stronger Password Requirements: User Attitudes and Behaviours, In *Proceedings of the Symposium on Usable Privacy and Security*, ACM, pp. 14-34.

Shepard, R. N. (1967). Recognition memory for words, sentences and pictures. *Journal of Verbal Learning and Verbal Behaviour*, 6, pp. 156-163.

Singh, C. and Singh L., (2011), Investigating the Combination of Text and Graphical Passwords for a more secure and usable experience*, International Journal of Network Security & Its Applications (IJNSA)*, 3(2), pp. 78-95.

Singh, S., Cabraal, A., Demosthenous, C., Astbrink, G. and Furlong, M. (2007). Password sharing: implications for security design based on social practice. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pp. 895-904

Siponen, M., Pahnila, S. and Mahmood, M. A. (2010). Compliance with information security policies: An empirical investigation. Computer, 43(2), pp. 64-71.

Smith, R. E. (2001). *Authentication: From Passwords to Public Keys*, Addison Wesley.

Smith, S. W. (2003). Humans in the loop: Human-computer interaction and security. *IEEE Security & privacy*, *99*(3), pp. 75-79.

Sobrado, L. and Birget, J. C. (2002). Graphical passwords. *The Rutgers Scholar, an electronic Bulletin for undergraduate research*,*4*.

Soltanmohammadi, S., Asadi, S. and Ithnin, N. (2013). Main human factors affecting information system security. *Interdisciplinary Journal of Contemporary Research in Business*, *5*(7), pp. 329-354.

Sreelatha, M., Shashi, M., Anirudh, M., Ahamer, M. and Manoj Kumar, V. (2011). Authentication Schemes for Session Passwords Using Color and Images. *International Journal of Network Security & Its Applications*, 3(3), pp.111-119.

Srisawang, S., Thongmak, M. and Ngarmyarn, A. (2015). Factors Affecting Computer Crime Protection Behaviour. In *PACIS*, p. 31.

Standing, L. (1973). Learning 10,000 pictures, *Quarterly journal of Experimental*, pp. 207-222.

Standing, L., Conezio, J. and Haber, R., (1970), Perception and memory for pictures: Singletrial learning of 2500 visual stimuli, *Psychonomic Science*, pp.73-74.

Stobert, E. (2014). The agony of passwords: Can we learn from user coping strategies?. In *Extended Abstracts on Human Factors in Computing Systems*. pp. 975-980.

Stone-Gross, B., Cova, M., Cavallaro, L., Gilbert, B., Szydlowski, M., Kemmerer, R., Kruegel, C. and Vigna G. (2009). Your botnet is my botnet: Analysis of a botnet takeover. In *Proceedings of the 16th Conference on Computer and Communications Security (CCS)*. ACM, pp. 635-647.

Summers, W. C. and Bosworth, E. (2004). Password Policy; The Good, The Bad and The Ugly, *In Proceedings of the Winter International Symposium on Information and Communication Technologies*, ACM, pp. 1-6.

Suo, X., Zhu, Y. and Owen, G. S. (2005). Graphical passwords: A survey. In *Proceedings of The 21st Annual Computer Security Applications Conference,* IEEE, Computer Society Washington, DC, USA, pp. 463 - 472.

Sutton, S. (1998). Predicting and Explaining Intentions and Behaviour: How Well Are We Doing? *Journal of Applied Social Psychology,* 28, pp. 1317-1338.

Tao, H. and Adams, C. 2008. Pass-Go: A Proposal to Improve the Usability of Graphical Passwords. *International Journal of Network Security, 7*, 273-292.

Thorpe, J. and van Oorschot, P. C. (2004). Towards secure design choices for implementing graphical passwords. In *Computer Security Applications Conference 20th Annual*, pp. 50-60

Thorpe, J. and van Oorschot, P. C. (2004). Graphical Dictionaries and the Memorable Space of Graphical Passwords. In *USENIX Security Symposium* pp. 135-150.

Thorpe, J., MacRae, B. and Salehi-Abari, A. (2013). Usability and security evaluation of geopass: A geographic location-password scheme, In *Proceedings of the Ninth symposium on usable privacy and security,* ACM, p. 14.

Topkara, U., Topkara, M. and Atallah, M. J. (2007). Passwords for Everyone: Secure Mnemonic-based Accessible Authentication. In *USENIX Annual Technical Conference*, pp. 369-374.

Ur, B., Kelley, P. G., Komanduri, S., Lee, J., Maass, M., Mazurek, M., Passaro, T., Shay, R., Vidas, T., Bauer, L., Christin, N. and Cranor, L. (2012). How does your password measure up? The effect of strength meters on password creation. In *USENIX Security Symposium*, pp. 65-80.

Ur, B., Noma, F., Bees, J., Segreti, S. M., Shay, R., Bauer, L. and Cranor, L. F. (2015). "i added '!'at the end to make it secure": Observing password creation in the lab. In *Proc. SOUPS*.

Van Oorschot, P. and Thorpe, J. (2011). Exploiting predictability in click-based graphical passwords*. *Journal of Computer Security*, 19(4), pp.669-702.

Van Oorschot, P. C. and Wan, T. (2009). TwoStep: An authentication method combining text and graphical passwords. In *International Conference on E-Technologies,* pp. 233-239

Vance, A., Suponen, M. and Pahnila. S. (2009). How Personality and Habit Affect Protection Motivation. In *Association of Information Systems SIGSEC Workshop on Information Security & Privacy (WISP'09),* Phoenix, AZ, USA, pp. 1-7

Vorster, J. and van Heerden, R. (2015a). *A Study of Perceptions of Graphical Passwords*. [online] ResearchGate. Available at: https://www.researchgate.net/publication/283712970_A_Study_of_Perceptions_of_Graphical_Passwords [Accessed 2 Jun. 2016].

Vorster, J. and van Heerden, R. (2015b). Graphical passwords: a qualitative study of password patterns. *The Proceedings of the 10th International Conference on Cyber Warfare and Security*, pp. 375-386.

Vu, K. P. L., Proctor, R. W., Bhargav-Spantzel, A., Tai, B. L. B., Cook, J. and Schultz, E. E. (2007). Improving Password Security and Memorability to Protect Personal and Organisational Information. *International Journal of Human-Computer Studies,* 65(8), pp. 744-757.

Weir, M., Aggarwal, S., Collins, M. and Stern, H. (2010). Testing metrics for password creation policies by attacking large sets of revealed passwords. In *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 162-175

Weirich, D. (2005). *Persuasive password security*, Ph.D., University College London.

Weirich, D. and Sasse, M. A. (2002). Pretty Good Persuasion: A First Step towards Effective Password Security in The Real World. In the *Proceedings of the 2001 Workshop on New Security Paradigms Workshop,* ACMPress, New York, USA, pp. 137-143.

Whitten, A. and Tygar, J. D. (1999). Why Johnny Can't Encrypt: A Usability Evaluation of PGP 5.0. In *Usenix Security Symposium.*

Wiedenbeck, S., Waters, J., Birget, J. C., Brodskiy, A. and Memon, N. (2005a). Authentication using graphical passwords: Effects of tolerance and image choice. In *Proceedings of the 2005 symposium on Usable privacy and security*, pp. 1-12.

Wiedenbeck, S., Waters, J., Birget, J.C., Brodskiy, A. and Memon, N. (2005b). *PassPoints: Design and longitudinal evaluation of a graphical password system*, International Journal of Human Computer Studies

Wilkes, M. V. (1968). Time-sharing computer systems. American Elseviser

Wood, D., Bruner, J. S. and Ross, G. (1976). The role of tutoring in problem solving. *Journal of child psychology and psychiatry*, *17*(2), pp. 89-100.

Woodhouse, S. (2007). Information Security: End User Behaviour and Corporate Culture, In Proceedings of *The 7th IEEE International Conference on Computer and Information Technology,* IEEE, Computer Society Washington, DC, USA, pp. 767-774.

Wright, N., Patrick, A. S. and Biddle, R. (2012). Do you see your password?: applying recognition to textual passwords. In *Proceedings of the Eighth Symposium on Usable Privacy and Security,* ACM, p. 8.

Xu, H., Rosson, M. B. and Carroll, J. M. (2007). Increasing the Persuasiveness of IT Security Communication: Effects of Fear Appeals and Self-View. In *Proceedings of the Symposium On Usable Privacy and Security,* pp. 18-20.

Yampolskiy, R.V. (2007). *Secure Network Authentication with Pass Text*, 4th International Conference on Information Technology: New Generations (ITNG 2007), pp. 831-836.

Yampolskiy, R.V. and Govindaraju, V. (2006). *Use of Behavioural Biometrics in Intrusion Detection and Online Gaming,* Biometric Technology for Human Identification III, SPIE Defense and Security Symposium, Orlando, Florida, USA.

Yan, J. J. (2001). A note on proactive password checking. In *Proceedings of the 2001 workshop on New security paradigms,* ACM, pp. 127-135.

Yan, J., Blackwell, A., Anderson, R. and Grant, A. (2004). Password Memorability and Security: Empirical Results. *IEEE Privacy & Security, 2*(5), pp. 25-31.

Zakaria, N. H. B. (2013). *Exploring human factors issues & possible countermeasures in password authentication*, Ph.D. Newcastle University.

Zhang-Kennedy, L., Chiasson, S. and Biddle, R. (2013). Password advice shouldn't be boring: Visualizing password guessing attacks. In *eCrime Researchers Summit (eCRS),* IEEE*,* pp. 1-11.

Zhang, L. and McDowell, C. W. (2009). Am I Really at Risk? Determinants of Online Users' Intention to Use Strong Passwords, *Journal of Internet Commerce*, (8), pp. 180-197.

Zhang, Y., Monrose, F. and Reiter, M. K. (2010). The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 176-186.

Zhao, H. and Li, X. (2007). S3PAS: A scalable shoulder-surfing resistant textual-graphical password authentication scheme. In *Advanced Information Networking and Applications Workshops, AINAW'07. 21st International Conference,* IEEE, Vol. 2, pp. 467-472.

Zheng, Z., Liu, X., Yin, L. and Liu, Z. (2010). A Hybrid Password Authentication Scheme Based on Shape and Text. *Journal of Computers*, 5(5).

Zurko, M. E. (2005). User-Centered Security: Stepping Up to the Grand Challenge. In *Proceedings of the Annual Computer Security Application Conference*, IEEE, Computer Society Washington, DC, USA, pp. 188-202.

Zviran, M. and Haga, W. J. (1990). Cognitive passwords: the key to easy access control. *Computers & Security*, 9(8), pp.723-736

Zviran, M., and Haga, W. J. (1993). Comparison of Password Techniques for Multilevel Authentication Mechanisms. *The Computer Journal*, 36(3), pp. 227-237.

LIST OF APPENDICES

APPENDIX A

MATERIALS RELATED TO THE FIRST EXPERIMENT

- **Certificate of Ethical Approval**

University of Sussex

Certificate of Approval	
Reference Number	ER/MY68/2
Title Of Project	Improving Password Security in Organizations
Principal Investigator (PI):	Ian Mackie
Student	Merve Yildirim
Collaborators	
Duration Of Approval	1 month
Expected Start Date	15-Aug-2016
Date Of Approval	05-Oct-2016
Approval Expiry Date	30-Oct-2016
Approved By	David Reby
Name of Authorised Signatory	
Date	05-Oct-2016

*NB. If the actual project start date is delayed beyond 12 months of the expected start date, this Certificate of Approval will lapse and the project will need to be reviewed again to take account of changed circumstances such as legislation, sponsor requirements and University procedures.

Please note and follow the requirements for approved submissions:

Amendments to protocol

* Any changes or amendments to approved protocols must be submitted to the C-REC for authorisation prior to implementation.

Feedback regarding the status and conduct of approved projects

* Any incidents with ethical implications that occur during the implementation of the project must be reported immediately to the Chair of the C-REC.

Feedback regarding any adverse and unexpected events

* Any adverse (undesirable and unintended) and unexpected events that occur during the implementation of the project must be reported to the Chair of the Social Sciences C-REC. In the event of a serious adverse event, research must be stopped immediately and the Chair alerted within 24 hours of the occurrence.

For Life Sciences and Psychology projects

* The principal investigator is required to provide a brief annual written statement to the committee, indicating the status and conduct of the approved project. These reports will be reviewed at the annual meeting of the committee. A statement by the PI to the C-REC indicating the status and conduct of the approved project will be required on the Approval Expiration Date as stated above.

- **Recruitment Letter**

Re: Improving Password Security in the Organisations

Dear <<insert name>>

As a doctoral researcher at University of Sussex, I am writing to invite you to participate in an academic study entitled "Improving Password Security in Organisations". I am specifically contacting you because of your wealth of expertise and experience in this area.

With this study, I aim to explore the reasons why employees are not motivated to protect their passwords against potential security failures within the organisation. There is a wealth of research demonstrating that, despite technical precautions taken by people within the organisation, undesired password-related behaviours cause organisations to lose confidential information.

In this study, I will be using some selected scientific methods and approaches to study employees' insecure password practices and persuade and motive them to behave in a more secure manner. To do this, firstly, underlying reasons that cause users' lack of engagement with password security should be investigated and suitable methods should be applied to prevent possible security failures. For this, I aim to conduct in-depth interviews and surveys with employees in different positions who use passwords to access organisational information in several organisations in Turkey.

Taking part in this research is optional but your extensive knowledge and experience in the field is highly valuable to the study. Enclosed you will find the Information Sheet and Consent Form, which contain more information about the study and your role, should you choose to participate. A follow-up email or a call will be made on <<date>> to answer any questions you might have about participating.

If you wish to opt out of future contact, please email the address at the top of this letter to request that no further contact be made. Agreement to be contacted or request for more information does not obligate you to participate in any study.

If you would like additional information about this study please email

M.Yildirim@sussex.ac.uk

Thank you for considering this research opportunity.

Best Regards,

Merve Yildirim

Doctoral Researcher

Department of Informatics Chichester 2

University of Sussex Brighton, BN1 9SJ, UK

- **Consent Form**

Project Title: Improving Password Security in Organisations

Researcher's Contact Details:

Merve Yıldırım

Doctoral Researcher

Department of Informatics

University of Sussex

Brighton, BN1 9SJ, UK

Email: M.Yildirim@sussex.ac.uk

Name of Participant .....

I agree to take part in the above University of Sussex research project. I have had the project explained to me and I have read and understood the Information Sheet, which I may keep for my records. I understand that agreeing to take part means that I am willing to:

- Be interviewed by the researcher; - Allow the interview to be audio taped; - Make myself available for a further interview should that be required. However, I am aware that the follow-up is by invitation only and I can refuse to take part at any stage without giving an explanation.

I understand that any information I provide is confidential, and that no information that I disclose will lead to the identification of any individual in the reports on the project, either by the researcher or by any other party.

I understand that I will have an option of seeing the transcript of data concerning me before it is included in the write up of the research.

I understand that I have given my approval for my role and position in the organisation where I work to be used in the final report of the project, and in further publications.

I understand that my participation is voluntary, that I can choose not to participate in part or all of the project, and that I can withdraw at any stage of the project without being penalised or disadvantaged in any way.

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with the UK Data Protection Act 1998.

Date:

Signature of the Researcher:

Signature of Participant:

- **The Questionnaire for non-IT Employees:**

1. Your institution?

2. Your job/position?

3. Does your job require you to use password?

4. Does your job require you to access any critical information?

5. Do you think you have enough knowledge about password security and your organisation's information security policy?

6. Has your password ever been hacked or have you ever encountered a situation that would threaten the security of your personal or company information by this time?

7. What do you do if your work password is hacked/ What have you done when your work password was hacked?

8. Does the authentication scheme you use at work direct you to choose strong passwords?

9. Do you share your work password with your colleagues?

10. Do you keep your work password somewhere accessible by others?

11. How often do you change your work password?

12. Do you use the same password for your work and personal accounts?

13. Which one do you care more to choose strong password?

- ☐ Your personal accounts
- ☐ Work accounts

14. What is the reason for your insecure password practices at work?

- ☐ usability issues of authentication mechanisms/password policy rules
- ☐ lack of password security education/awareness
- ☐ that you do not believe the importance of password security
- ☐ workload
- ☐ personal reasons
- ☐ other (please specify)

15. Have you attended any education/training program about password/information security at work?

If yes,

- What was the content of education?

- Was it given by an expert?

- How useful was it?

16. What would motivate you to change your insecure password practices at work and adopt the secure ones?

- ☐ Being punished for the insecure practices
- ☐ Being rewarded for the good practices
- ☐ Usable password mechanisms

- ☐ Your colleagues' good password practices
- ☐ Your awareness about the consequences of password failures
- ☐ Personal beliefs on importance of information privacy

- **The Interview Questions for It Specialists**

1. Your institution?

2. Your job/position?

3. Can you please mention about your organisation's password security regulations?

4. How is the employee's password selection process in your organisation? Do the employees create passwords themselves or do they use system-generated passwords?

5. What kind of measures does your organisation take to ensure password security?

6. Do you think that the authentication scheme you use at work directs employees to choose strong passwords?

7. Is there any password meter measuring the strength of passwords integrated into the system which can be used by employees when they create their passwords?

8. Which one do you think threaten the password security most at work?

- ☐ Technical issues
- ☐ Insecure password practices

9. Have the employees in your organisation been given any password security education?

10. Do you think the measures taken for the password security of your organisation is sufficient? What would you suggest for a better security as an expert?

APPENDIX B

MATERIALS RELATED TO THE SECOND EXPERIMENT

- ## Certificate of Ethical Approval

University of Sussex

Certificate of Approval	
Reference Number	ER/MY68/1
Title Of Project	Persuading Users to Create Stronger Passwords
Principal Investigator (PI):	Ian Mackie
Student	Merve Yildirim
Collaborators	
Duration Of Approval	2 months
Expected Start Date	29-Feb-2016
Date Of Approval	02-Mar-2016
Approval Expiry Date	29-Apr-2016
Approved By	David Reby
Name of Authorised Signatory	
Date	02-Mar-2016

*NB. If the actual project start date is delayed beyond 12 months of the expected start date, this Certificate of Approval will lapse and the project will need to be reviewed again to take account of changed circumstances such as legislation, sponsor requirements and University procedures.

Please note and follow the requirements for approved submissions:

Amendments to protocol

* Any changes or amendments to approved protocols must be submitted to the C-REC for authorisation prior to implementation.

Feedback regarding the status and conduct of approved projects

* Any incidents with ethical implications that occur during the implementation of the project must be reported immediately to the Chair of the C-REC.

Feedback regarding any adverse and unexpected events

* Any adverse (undesirable and unintended) and unexpected events that occur during the implementation of the project must be reported to the Chair of the Social Sciences C-REC. In the event of a serious adverse event, research must be stopped immediately and the Chair alerted within 24 hours of the occurrence.

For Life Sciences and Psychology projects

* The principal investigator is required to provide a brief annual written statement to the committee, indicating the status and conduct of the approved project. These reports will be reviewed at the annual meeting of the committee. A statement by the PI to the C-REC indicating the status and conduct of the approved project will be required on the Approval Expiration Date as stated above.

- **Recruitment Letter**

Re: Persuading Users to Create Stronger Passwords

Hello,

My name is Merve and I am a PhD student at the Department of the Informatics at the University of Sussex. I am planning to invite students to participate in an academic study on improving password security through persuasion strategies as part of my PhD work.

I am doing this research to explore the reasons of students' unsecure password practices and motive them to create strong and memorable passwords. To do this, I need participants to sign in the website (link is provided below) and fill the questionnaire.

If you would like additional information about this study, please email me at M.Yildirim@sussex.ac.uk Request for more information does not obligate you to participate in any study.

Taking part in this research is optional but your participation would be very helpful. If you decide to join, please access the project's web site through this link <<website's link>>. Please remember that your participation can provide you beneficial information which you can use to produce stronger passwords in your daily life.

Thank you for helping this research.

Best Regards,

Merve Yildirim

Doctoral Researcher

Department of Informatics Chichester 2

University of Sussex Brighton, BN1 9SJ, UK

- **Consent Form**

Project Title: Persuading Users to Create Stronger Passwords

Researcher's Contact Details:

Merve Yıldırım

Doctoral Researcher

Department of Informatics

University of Sussex

Brighton, BN1 9SJ, UK

Email: M.Yildirim@sussex.ac.uk

Participant's Declaration:

I agree to take part in the above University of Sussex research project. I have had the project explained to me and I have read and understood the Information Sheet, which I may keep for records.

I understand that any information I provide is confidential, and that no information that I disclose will lead to the identification of any individual in the reports on the project, either by the researcher or by any other party.

I understand that I have given my approval for the name of my town/community and / or the name of my workplace to be used in the final report of the project, and in further publications.

I understand that my participation is voluntary, that I can choose not to participate in part or all of the project, and that I can withdraw at any stage of the project without being penalised or disadvantaged in any way.

I consent to the processing of my personal information for the purposes of this research study. I understand that such information will be treated as strictly confidential and handled in accordance with the Data Protection Act 1998.

Date:

Signature of the Researcher:

- **Common Survey Questions for the Control and the Experimental Group**

Your age?

❑ Less than 18 years
❑ 18-25 years
❑ 26-35 years
❑ 36-55 years
❑ More than 55 years

Your gender?
❑ Female
❑ Male

Your current university?

Your current course/degree?
❑ Undergraduate (BA, BSc etc.)
❑ Postgraduate (MA, MSc, PhD, Postdoc etc.)

Your faculty?
❑ Science, Agriculture and Engineering
❑ Humanities & Social Sciences
❑ Medical Sciences

Do you have a degree in computer science, information technology, computer engineering or a related field?
❑ Yes
❑ No

Have you ever had any password security failure experience?
❑ Yes, my password has been hacked or stolen at least once in my life.
❑ No, I have not had any password security failure experience.

Have you ever written down your passwords and kept them somewhere easily accessible?
❑ Yes, I write down my passwords somewhere accessible (on a notebook etc.).
❑ No, I write down my passwords somewhere safe (in a file which is encrypted etc.).
❑ I never write down my passwords as I keep them in my mind.

Have you ever shared your passwords with someone else?
❑ Yes, I share my passwords with others.
❑ Yes, I share my password only with my family and friends.
❑ I share my passwords only if I have to.
❑ No, I never share my passwords with anyone.

Have you ever reused your passwords?

- ☐ Yes, I use the same password for different accounts.
- ☐ Not exactly the same one but I use similar passwords for different accounts.
- ☐ No, I never use same the password for different accounts.

For which account(s) do you care to choose strong passwords?

- ☐ For all my accounts
- ☐ For all websites
- ☐ For my personal email accounts
- ☐ For social networking sites (facebook, twitter etc.)
- ☐ For online banking
- ☐ For online shopping
- ☐ For online booking
- ☐ For the accounts which hold my credit card information (PayPal etc.)
- ☐ For my work emails
- ☐ None of them

How do you normally create your passwords?

- ☐ Dictionary words or meaningful details (name, birth date, team you support, flower name, phone number etc.)
- ☐ Combination of meaningful details (Sharon1978 etc.)
- ☐ Common passwords (password123 etc.)
- ☐ Common patterns (12345, qwerty etc.)
- ☐ Mixing keyboard characters with words (p@ssw0rd etc.)
- ☐ Random combination of characters (Th7&3.?we etc.)
- ☐ Other
- ☐ I prefer not to answer.

If you try to choose strong passwords which rules would you apply?

- ☐ At least 8-character long
- ☐ Including lower case letters
- ☐ Including upper case letters
- ☐ Including special keyboard characters
- ☐ Passwords which don't contain name, surname, birthday etc.
- ☐ Passwords which don't contain meaningful words
- ☐ Passwords which don't contain common patterns (password, 12345 etc.)
- ☐ I would not use any rules.
- ☐ I prefer not to answer.

What do you think about password policy rules (at least 8 characters long, including upper case and special keyboard characters etc.)?

- ☐ I don't find them useful and necessary. I don't like to apply them.
- ☐ Password creation rules make it difficult creating my passwords. It is annoying and time consuming so I don't like to apply them.
- ☐ I believe they make my passwords stronger but still I don't like to apply them.
- ☐ I find them useful and I believe they increase the security level. I like to apply them.

Do you think your passwords are hard to crack or guess?
❑ Yes, I think my passwords are strong enough.
❑ No, I do not think my passwords are strong enough.

Do you use password manager or browser extension to store your passwords in order to avoid forgetting them?
❑ Yes, I use password manager to store my passwords.
❑ Yes, I use browser extension to store my passwords.
❑ No, I don't use any program to store my passwords.

Do you use any authentication mechanism other than traditional passwords such as graphical passwords or biometrics?
❑ Yes, I use graphical passwords.
❑ Yes, I use token based authentication systems.
❑ Yes, I use biometrics.
❑ Yes, I use one time passwords (SMS based etc.).
❑ No, I only use traditional text-based passwords.

Is the password you have just created for this website that you have used in the past?
❑ Yes, I used this password before.
❑ No, I did not use this password before.
❑ Not exactly the same one but I used a similar password before.
❑ I prefer not to answer.

- **Specific Survey Questions for The Experimental Group**

Have you used the given methods to create your password for this website?
❑ Yes, I have used the first method. I have specified a formula and used it to turn an ordinary word to a strong password.
❑ Yes, I have used the second method. I have mixed a number and a string thus created a strong password.
❑ Yes, I have used the third method. I have picked several meaningful words and combined them with keyboard characters thus created a very long and strong password.
❑ No, I have not used any method to create the password.

Do you think the given methods are useful and they help you to create stronger and memorable passwords?
❑ Yes, they are useful and helpful to create strong passwords.
❑ No, they are not useful and helpful to create strong passwords.

Applying the given methods to create password was easy.
To what extent do you agree or disagree?
❑ Strongly agree

❑ Agree
❑ Neutral
❑ Disagree
❑ Strongly disagree

Applying the given methods to create password was fun.
To what extent do you agree or disagree?
❑ Strongly agree
❑ Agree
❑ Neutral
❑ Disagree
❑ Strongly disagree

Creating strong and memorable passwords is worth the time and effort spent to apply the given methods.
To what extent do you agree or disagree?
❑ Strongly agree
❑ Agree
❑ Neutral
❑ Disagree
❑ Strongly disagree

How likely do you think you will be able to remember the password you created for this website after a week and a month?
After a week
❑ Very likely
❑ Likely
❑ About as likely as not
❑ Unlikely
❑ Very unlikely
After a month
❑ Very likely
❑ Likely
❑ About as likely as not
❑ Unlikely
❑ Very unlikely

Do you think the given methods and advice persuaded you not to write down your passwords?
❑ Yes, I think so.
❑ No, I do not think so.

Do you think the given methods and advice persuaded you not to share your passwords?
❑ Yes, I think so.
❑ No, I do not think so.

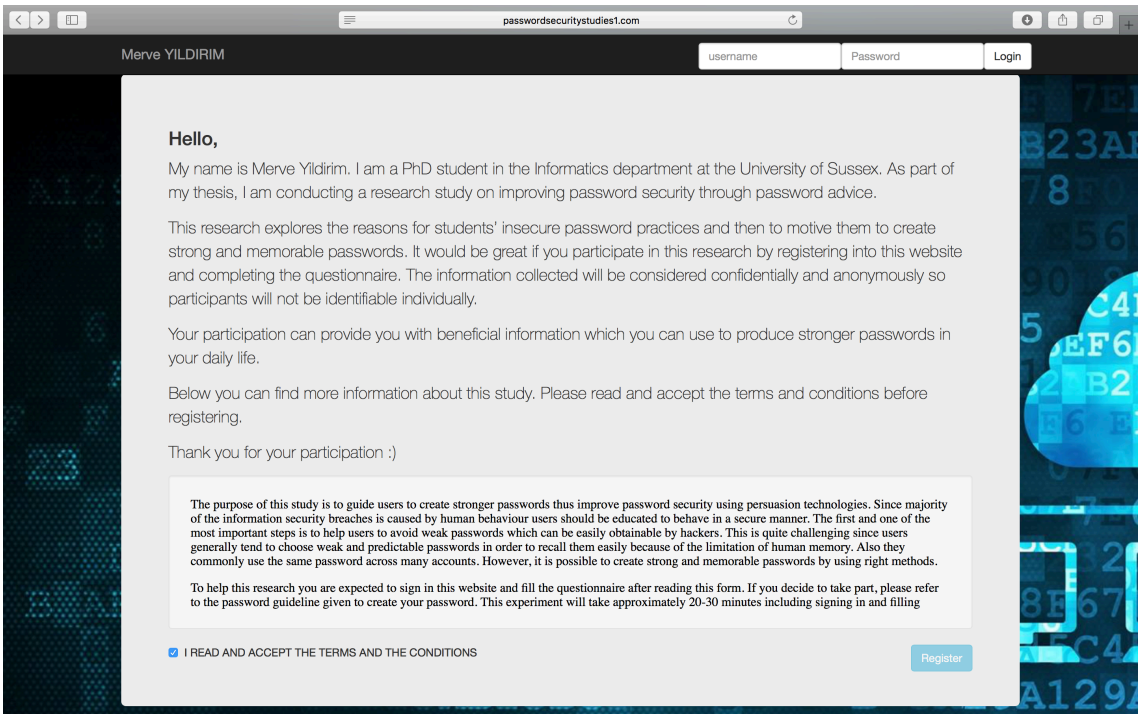
Do you think the given methods and advice persuaded you not to reuse your passwords?
❑ Yes, I think so.
❑ No, I do not think so.

I think applying the given methods to create strong and memorable passwords is much more efficient than following strict password policy rules.
To what extent do you agree or disagree?
☐ Strongly agree
☐ Agree
☐ Neutral
☐ Disagree
☐ Strongly disagree

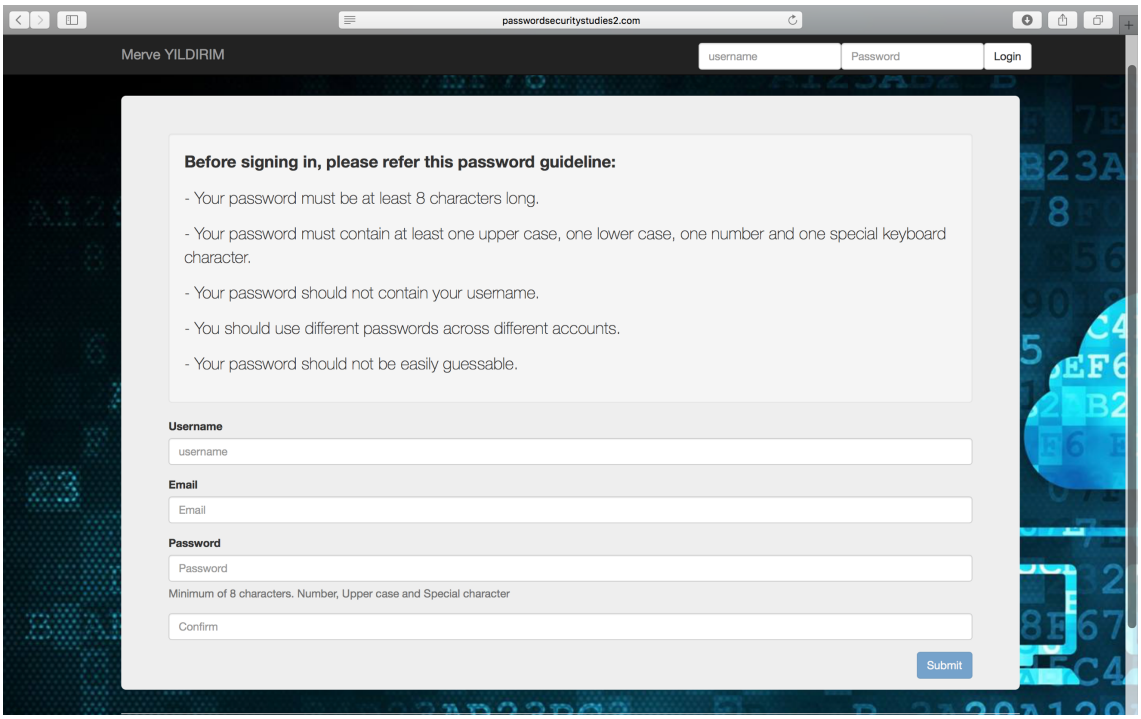
Will you use the given methods and advice while creating passwords in future?
☐ Yes, I will use them.
☐ No, I will not use them.

What would you recommend to improve password security?

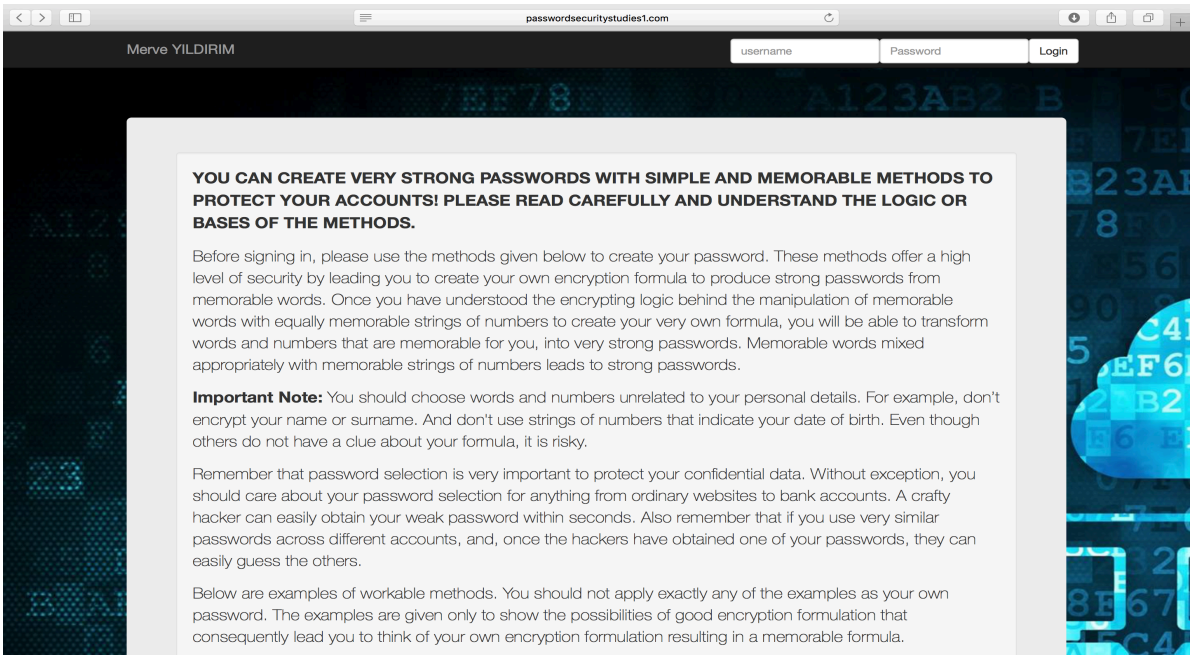
- **Information Page for the Participants**

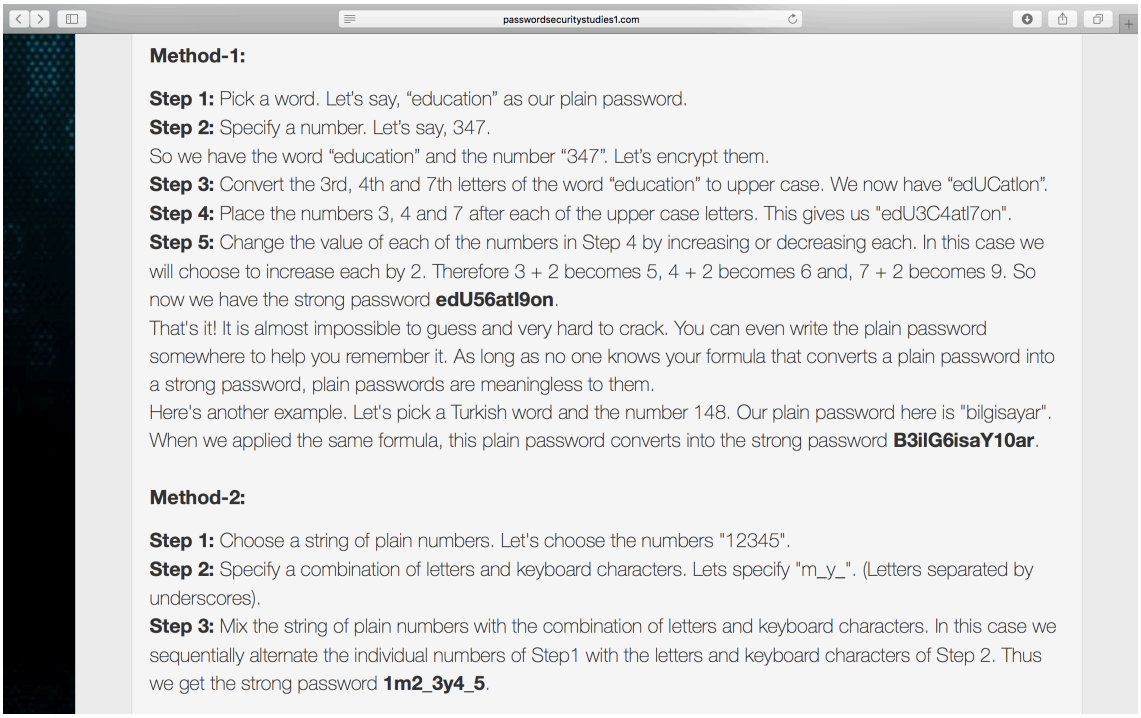


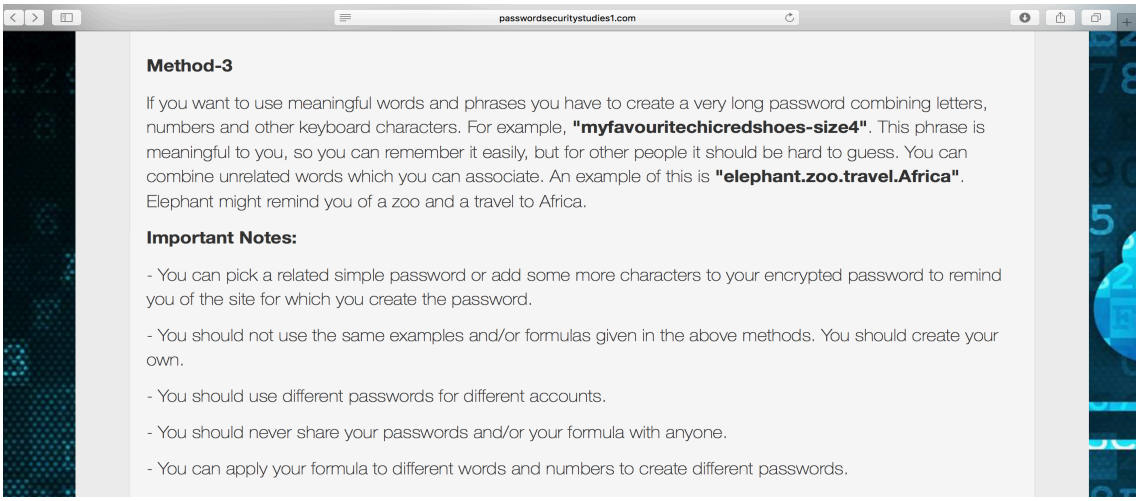
- **Sign in / Login Page for The Control Group**

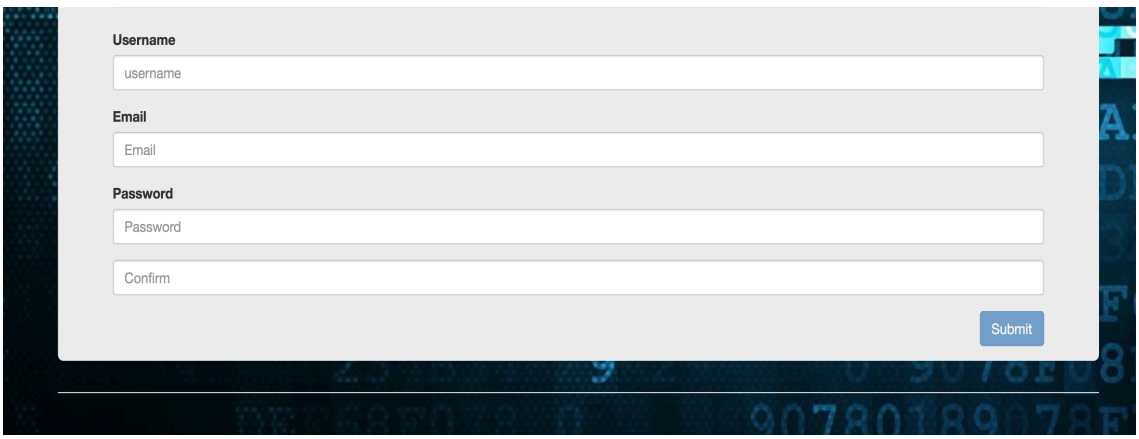


- **Sign in / Login Page for The Experimental Group**




passwordsecuritystudies1.com
Method-1:
Step 1: Pick a word. Let's say, "education" as our plain password.
Step 2: Specify a number. Let's say, 347.
So we have the word "education" and the number "347". Let's encrypt them.
Step 3: Convert the 3rd, 4th and 7th letters of the word "education" to upper case. We now have "edUCatIon".
Step 4: Place the numbers 3, 4 and 7 after each of the upper case letters. This gives us "edU3C4atI7on".
Step 5: Change the value of each of the numbers in Step 4 by increasing or decreasing each. In this case we will choose to increase each by 2. Therefore 3 + 2 becomes 5, 4 + 2 becomes 6 and, 7 + 2 becomes 9. So now we have the strong password edU56atI9on.
That's it! It is almost impossible to guess and very hard to crack. You can even write the plain password somewhere to help you remember it. As long as no one knows your formula that converts a plain password into a strong password, plain passwords are meaningless to them.
Here's another example. Let's pick a Turkish word and the number 148. Our plain password here is "bilgisayar". When we applied the same formula, this plain password converts into the strong password B3ilG6isaY10ar.
Method-2:
Step 1: Choose a string of plain numbers. Let's choose the numbers "12345".
Step 2: Specify a combination of letters and keyboard characters. Lets specify "m_y_". (Letters separated by underscores).
Step 3: Mix the string of plain numbers with the combination of letters and keyboard characters. In this case we sequentially alternate the individual numbers of Step1 with the letters and keyboard characters of Step 2. Thus we get the strong password 1m2_3y4_5.


passwordsecuritystudies1.com
Method-3
If you want to use meaningful words and phrases you have to create a very long password combining letters, numbers and other keyboard characters. For example, "myfavouritechicredshoes-size4". This phrase is meaningful to you, so you can remember it easily, but for other people it should be hard to guess. You can combine unrelated words which you can associate. An example of this is "elephant.zoo.travel.Africa". Elephant might remind you of a zoo and a travel to Africa.
Important Notes:
- You can pick a related simple password or add some more characters to your encrypted password to remind you of the site for which you create the password.
- You should not use the same examples and/or formulas given in the above methods. You should create your own.
- You should use different passwords for different accounts.
- You should never share your passwords and/or your formula with anyone.
- You can apply your formula to different words and numbers to create different passwords.


Username
username
Email
Email
Password
Password
Confirm
Submit

- **Password Strength Measurement Tool**

Test Your Password		Minimum Requirements
Password:		• Minimum 8 characters in length • Contains 3/4 of the following items: - Uppercase Letters - Lowercase Letters - Numbers - Symbols
Hide:	☑	
Score:	0%	
Complexity:	Too Short	

Additions		Type	Rate	Count	Bonus
✗	Number of Characters	Flat	*+(n*4)*	0	0
✗	Uppercase Letters	Cond/Incr	*+((len-n)*2)*	0	0
✗	Lowercase Letters	Cond/Incr	*+((len-n)*2)*	0	0
✗	Numbers	Cond	*+(n*4)*	0	0
✗	Symbols	Flat	*+(n*6)*	0	0
✗	Middle Numbers or Symbols	Flat	*+(n*2)*	0	0
✗	Requirements	Flat	*+(n*2)*	0	0
Deductions					
✓	Letters Only	Flat	*-n*	0	0
✓	Numbers Only	Flat	*-n*	0	0
✓	Repeat Characters (Case Insensitive)	Comp	-	0	0
✓	Consecutive Uppercase Letters	Flat	*-(n*2)*	0	0
✓	Consecutive Lowercase Letters	Flat	*-(n*2)*	0	0
✓	Consecutive Numbers	Flat	*-(n*2)*	0	0
✓	Sequential Letters (3+)	Flat	*-(n*3)*	0	0
✓	Sequential Numbers (3+)	Flat	*-(n*3)*	0	0
✓	Sequential Symbols (3+)	Flat	*-(n*3)*	0	0

APPENDIX C

MATERIALS RELATED TO THE THIRD EXPERIMENT

- Certificate of Ethical Approval

University of Sussex

Certificate of Approval	
Reference Number	ER/MY68/3
Title Of Project	Evaluation of Security and Usability of a Novel User Authentication Scheme Integrating Text and Graphical Passwords
Principal Investigator (PI):	Ian Mackie
Student	Merve Yildirim
Collaborators	
Duration Of Approval	1 month
Expected Start Date	14-Dec-2016
Date Of Approval	13-Dec-2016
Approval Expiry Date	23-Dec-2016
Approved By	David Reby
Name of Authorised Signatory	
Date	13-Dec-2016

*NB. If the actual project start date is delayed beyond 12 months of the expected start date, this Certificate of Approval will lapse and the project will need to be reviewed again to take account of changed circumstances such as legislation, sponsor requirements and University procedures.

Please note and follow the requirements for approved submissions:

Amendments to protocol

* Any changes or amendments to approved protocols must be submitted to the C-REC for authorisation prior to implementation.

Feedback regarding the status and conduct of approved projects

* Any incidents with ethical implications that occur during the implementation of the project must be reported immediately to the Chair of the C-REC.

Feedback regarding any adverse and unexpected events

* Any adverse (undesirable and unintended) and unexpected events that occur during the implementation of the project must be reported to the Chair of the Social Sciences C-REC. In the event of a serious adverse event, research must be stopped immediately and the Chair alerted within 24 hours of the occurrence.

For Life Sciences and Psychology projects

* The principal investigator is required to provide a brief annual written statement to the committee, indicating the status and conduct of the approved project. These reports will be reviewed at the annual meeting of the committee. A statement by the PI to the C-REC indicating the status and conduct of the approved project will be required on the Approval Expiration Date as stated above.

- **Recruitment Letter**

Re: Evaluation of Security and Usability of a Novel User Authentication Scheme Integrating Text and Graphical Passwords

Hello,

My name is Merve and I am a PhD student in the Department of Informatics. As part of my PhD study, I am planning to evaluate security and usability of a novel authentication scheme integrating text and graphical passwords. To do this, I need participants to try this new authentication scheme.

Neither knowledge of computer security nor experience with graphical passwords is required for the experiment. It only takes 10-15 minutes and should be fun and useful to participate.

The experiment will take place at **Chichester 2 2R306** between **14th December and 23th December 2016**. You can choose to come any time **between 10.00 am and 6.00 pm** to join the experiment. You will also have free chocolate and drink for joining the experiment.

I will look forward to hearing from you. If you are interested in participating, please email M.Yildirim@sussex.ac.uk

Many thanks.

Best Regards, Merve Yildirim

Doctoral Researcher

Department of Informatics

Chichester 2 2R306

University of Sussex Brighton, BN1 9SJ, UK

- **Consent Form**

Project Title: Evaluation of Security and Usability of a Novel User Authentication Scheme Integrating Text and Graphical Passwords

Researcher's Contact Details:

Merve Yıldırım

Doctoral Researcher

Department of Informatics

University of Sussex

Brighton, BN1 9SJ, UK

Email: M.Yildirim@sussex.ac.uk

Name of Participant .....

I agree to take part in the above University of Sussex research project. I have had the project explained to me and I have read and understood the Information Sheet, which I may keep for my records. I understand that agreeing to take part means that I am willing to:

1. Create a password and login the mobile application of the novel authentication scheme using the mobile phone provided by the researcher.

2. Allow the researcher to make some measurements (measuring login time etc.) during the experiment.

3. Complete a short questionnaire including questions about user satisfaction, efficiency and usability of the new authentication scheme after I test the scheme.

I understand that any information I provide is confidential, and that no information that I disclose will lead to the identification of any individual in any reports of the project, either by the researcher or by any other party.

I understand that I have given my approval for the experimental data I provided to be used in the final report of the project, and in further publications.

I understand that my participation is entirely voluntary so I can refuse to complete any task, and I can withdraw at any stage of the experiment without being penalised or disadvantaged in any way. I can also stop at any time and ask the researcher any questions I may have.

I have read the above information. All of my questions regarding the experimental procedure have been answered to my satisfaction.

I consent to participate in this research study. I understand that my personal information will be treated as strictly confidential and handled in accordance with the UK Data Protection Act 1998.

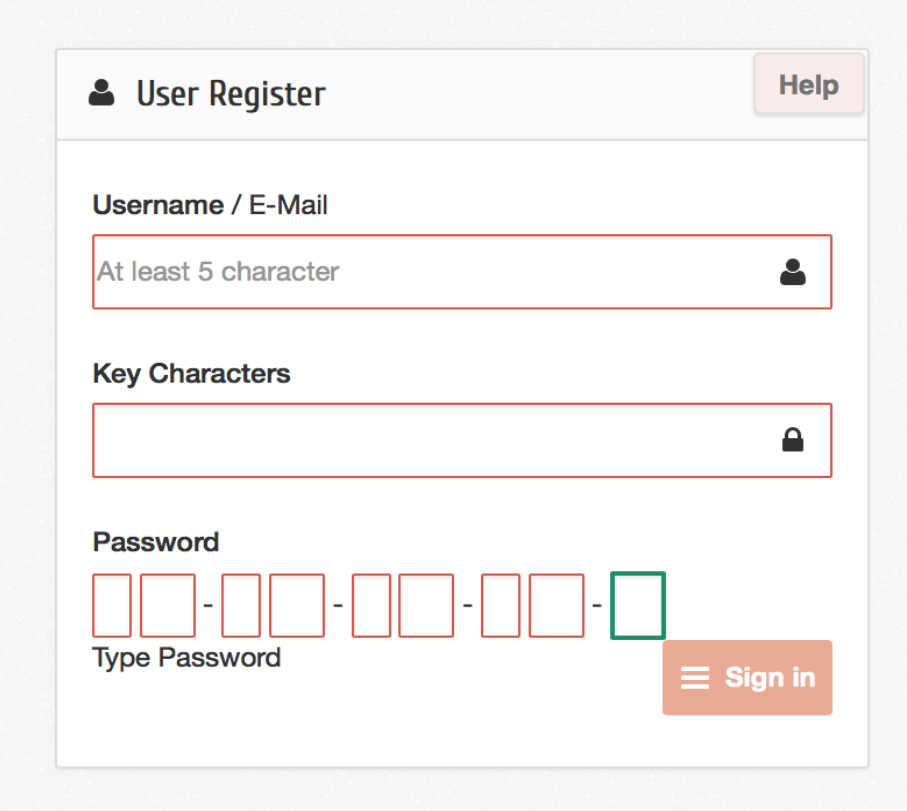
I confirm that I am 18 years of age or older.

Date:

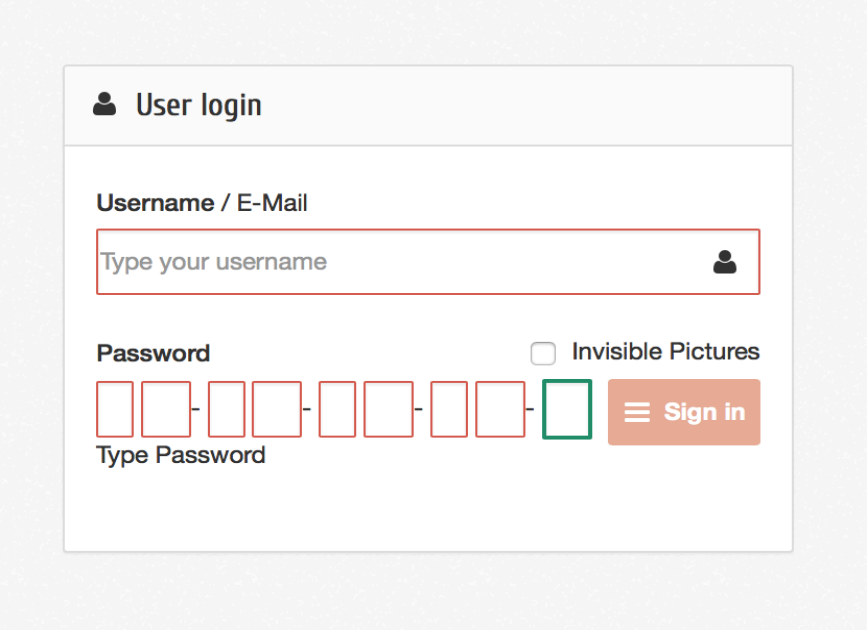
Signature of the Researcher:

Signature of Participant:

- **Sign in Page of the Implemented Authentication Scheme**



- **Login Page of the Implemented Authentication Scheme**



- **Survey Questions for the Participants**

Do you think it is easy to create a password using the new authentication scheme?
- ☐ Yes
- ☐ No

Do you think it is fun to create a password using the new authentication scheme?
- ☐ Yes
- ☐ No

Did you like the new authentication scheme?
- ☐ Yes
- ☐ No

Do you think it will help you to create stronger passwords?
- ☐ Yes
- ☐ No

Do you think it will help you to create memorable passwords?
- ☐ Yes
- ☐ No

Do you prefer to use the new authentication scheme to create passwords for all your accounts or only the important ones (bank account e.g.)?
- ☐ I prefer to use it for the all passwords
- ☐ I prefer to use it only for the important passwords
- ☐ I do not prefer to use it at all.